SAFETY ALERT 2020-05

Issue 01

Date of Issue: April 20, 2020

SUBJECT:
AIRCRAFT NETWORK SECURITY PROGRAM (ANSP)

REFERENCE PUBLICATIONS:
- Car Part VII Aviation Security Regulations
- Safety Alert 2017-09 Developing Cyber-Resilience Within The UAE Civil Aviation System
- Design Approval Holders (DAH) published guidance materials for e-Enabled Aircraft ANSP
- AC 121-7-2 (Rev 0) - Aircraft Network Security Program (ANSP) (Civil Aviation Authority of Singapore)
- AC 119-1 Operational Authorization of Aircraft Network Security Program (ANSP) (FAA)

BACKGROUND:
With the advancement of technology in the aircraft design, aircraft network connectivity has become a reality to facilitate aircraft operations and business needs. However at the same time this has resulted into the introduction of new vulnerabilities that may open access to on-board aircraft systems and may impede their operations, creating safety threats and business concerns. The new vulnerabilities, hence creation, necessitate the need for an ANSP development by the Air Operator to ensure proper control during software handling/distribution and network security on-board the aircraft.

The ANSP starts from the point whereby the software vendor/supplier transmits the software electronically (via internet) to the Air Operator and from the Air Operator through the wireless network or maintenance laptop to the aircraft.

This Safety Alert is applicable to an Aircraft Operator operating 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.

This safety alert is issued to:
a) Alert Air Operators about the obligation to develop and maintain an ANSP as and when required by the Design Approval Holder (DAH).
b) Provide guidance to demonstrate compliance with DAH requirement with regards to aircraft network security programme.

Note: the need for such ANSP will be considered for incorporate into next revision of CAR-OPS / CAR M.

RECOMMENDATIONS:

ACTION:

c) The Air Operator should ensure that an ANSP is developed and it is sufficiently comprehensive in scope and detailed enough to comply with the provisions in the following process.

d) Air Operator is ultimately responsible for the ANSP and as such ANSP should remain under its oversight.

PROCESS:

a) An ANSP should be developed and maintained for each applicable aircraft[1] to protect the usability, reliability, integrity, and safety of the network and data installed on an aircraft.

b) The ANSP should be sufficiently comprehensive in scope and detailed to accomplish the following:
   1) Ensure that aircraft ANSP is developed based on the DAH Aircraft Network Security Guidance (ANSOG) Document and is revised whenever there is a revision to the document.
   2) Ensure that data security protection is sufficient to prevent access by unauthorized devices or personnel external to the aircraft.
   3) Ensure that security threats specific to the operations are identified and are assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft (Appendix 2 refers).
   4) Ensure that security logs extracted from the aircraft's core network are continuously analysed and stored as specified by a SC or DAH manuals to better understand normal system behaviour and identify security risks to an extent consistent with their operational/threat profile.
   5) Prevent inadvertent or malicious changes to the aircraft network, including those possibly caused by maintenance activity.
   6) Prevent unauthorized access to the on-board network systems from sources on board the aircraft.

c) For each applicable aircraft, an ANSP document/manual should include the elements listed in Appendix 1.

d) The introduction of the ANSP necessitates close working relationship between aircraft avionics engineering and information technology (IT) security departments, therefore the Air Operator should review how engineering cooperate with IT for the management of ANSP.

e) The Air Operator should appoint a Data Security Manager by position, who acts as the administrator for the entire ANSP process with responsibilities listed under Appendix 3.

f) The Air Operator Quality Assurance/Compliance Monitoring Section review the developed ANSP and confirm that it address all applicable requirements in the DAH network security guidance documents.

g) The Air Operators conducts compliance monitoring of the ANSP to verify compliance with the program and to identify threats to the overall system. An integral part of this surveillance is to analyse threats and report them in a form and manner that is consistent with the IT security policies.

h) Any occurrences identified as threats should be reported to the GCAA reporting platforms.

CONTACTS:

Email: airworthiness@gcaa.gov.ae

[1] Applicability is determined by the Certification Basis of the aircraft as contained in the TCDS or STC data package.

APPENDIX 1: ELEMENTS TO BE PART OF THE ANSP MANUAL

a) Description of the aircraft security network, including the critical areas of the aircraft.
b) Duties and responsibilities for the ANSP, including persons with authority and responsibility for the safety objective in this alert and the person appointed as Data Security Manager;
c) Qualifications and Training for the personnel responsible for the safety objective in the alert including IT personnel who should possess skills requisite for accomplishing IT risk assessments that are traceable to industry standards. Training will vary depending on the level of involvement of each personnel;
d) Control of maintenance laptop/ground support equipment (GSE) access and use. The equipment should meet the DAH specifications. Strict physical and configuration controls should be implemented for the equipment related to the ANSP. Procedures for reporting lost equipment or equipment that may have been unaccounted for should be in the ANSP. Additionally, the ANSP should prohibit the use of personal data storage devices for transferring data intended for an aircraft or system related to the ANSP. Only operator-approved storage devices should be used to ensure secure transmission;
e) Activities related to the ANSP such as the scheduled data integrity and software conformity checks to aircraft assigned maintenance laptop/GSE restoration should be added to the maintenance program;
f) Control of access to airport wired and wireless service network;
g) Controlling access to Loadable Software Airplane Part (LSAP) librarian resource;
h) Creating secure parts signing processes and controlling access to private keys;
i) Control of aircraft conformity to type design. Changes made to the software configuration on the aircraft are treated with the intent as physical parts and require the issue of a Certificate of Release to Service;
j) Provisions for parts pooling and parts borrowing;
k) Procedures for part exchanges within its own fleet;
l) Event recognition and response;
m) Event evaluation process with considerations for program improvement; and
n) Security Environment Description.

APPENDIX 2

THE THREATS:

A successful attack can have an adverse effect on the aircraft and its occupants. Threats can cause a wide variety of failures

General Threat Identifiers	Aircraft Data Network Threats	Example of operational impact
Failure	Safe state of the aircraft system could be compromised in the event of security penetration	Access to flight controls by unauthorized individuals affecting safety
Denial	Aircraft system resources exhausted due to denial of service attack, system error, malicious actions	Critical services disrupted by system overload or traffic jamming
Access Control	Individual other than an authorized user may gain access to the aircraft system via an un-authorized controller, masquerade, spoofing system error or an attack for malicious purposes	Un-authorized Access
Passive Attack	Snooping or eavesdropping compromising security (misdirection). Flaws in security policies may lead to back door access	Un-authorized corruption or destruction of data causing unsafe flight conditions

Types of Failures

APPENDIX 3

THE DATA SECURITY MANAGER MAY BE RESPONSIBLE FOR THE FOLLOWING:

a) Manage any lost or stolen Ground Support Equipment (GSE) devices that are required for changing aircraft software configuration.
b) Create and control authorised user accounts.
c) Decommission equipment or parts in a way that no data is recoverable from them.
d) Provide logs, reports or other data to GCAA as required.
e) Maintain a password management programme for users.
f) Maintain records for equipment usage.
g) Restrict any services, protocols, connections or nodes that are not required.
h) Control access and utilisation for associated hardware required for aircraft network security programme.
i) Quarantine any crates or files that contain invalid digital signatures, until there is a way of verifying the contents are authorised. Any invalidated crates should be deleted.
j) Control of any cryptographic keys used in aircraft network security programme.
k) Control of any aircraft network security programme certificate expiration dates.
l) Identify and obtain aircraft software applications required for maintenance or modification of the aircraft configuration.
m) Verify software applications and identify any issues with associated hardware used for their installation.
n) Ensure suitable staging of software parts that will change aircraft configuration in a secure area, prior to installation on aircraft by appropriately licensed maintenance engineers.
o) Retain and monitor aircraft network security programme logs.
p) Retain any changes to the aircraft configuration
q) Keep track of any changes required by the authorised manufacturer's software security processes.
r) Update digital signatures if required for aircraft network security programme.
s) Monitor any expiration of digital signatures.
t) Eliminate any viruses or other malware that could affect the aircraft and/or systems required for the aircraft configuration.