SAFETY ALERT 2020-05

Issue 02

Date of Issue: November 22, 2020

SUBJECT:
AIRCRAFT NETWORK CYBER SECURITY PROGRAM (ANCSP)

REFERENCE PUBLICATIONS:
a) Car Part VII Aviation Security Regulations
b) Safety Alert 2017-09 Developing Cyber-Resilience Within The UAE Civil Aviation System
c) Type Certificate Holder (TCH)/Design Approval Holders (DAH) published guidance materials for ANSP
d) AC 121-7-2 (Rev 0) - Aircraft Network Security Program (ANSP) (Civil Aviation Authority of Singapore)
e) 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 ANCSP development by the Air Operator to ensure proper control during software handling/distribution in the ground support systems/equipment and network security on-board the aircraft.

The ANCSP 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 concerned by one or more of the following:

a) The Aircraft Type Certificate Holder (TCH)/Manufacturer publishing a specific aircraft Network Security Operator Guidance,
b) An ANCSP is identified by a Special Condition (SC) listed on the Type Certificate Data Sheet (TCDS) or,
c) If later modified, the requirement is identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC) with a SC.

Note: The term ANSP (for Aircraft Network Security Program) may be used by other regulatory agencies and TCH/DAH, it is usually equivalent to the term ANCSP used in this Safety Alert.

This safety alert is issued to:

a) Alert Air Operators about the obligations to develop and maintain an ANCSP as and when required by the TCH/the Design Approval Holder (DAH).
b) Provide guidance to demonstrate compliance with TCH/DAH requirements with regards to Aircraft Cyber Security Programme (ANCSP).

RECOMMENDATIONS

ACTION:

a) The Air Operator should ensure that an ANCSP is developed and it is sufficiently comprehensive in scope and detailed enough to comply with the provisions and the processes described in this Safety Alert.
b) Air Operator is ultimately responsible for the ANCSP and as such ANCSP should remain under its oversight, and
c) The Air operator should designate a person responsible for implementing and maintaining the ANCSP; that person may not necessarily be part of CAMO and CAR-OPS organisations;
d) The Air Operator should demonstrate compliance with the requirements in this Safety Alert within six (6) months after the effective date of this issue. Therefore, a compliance plan with the requirements in the SA shall be developed and presented to the GCAA CAR-M PAI and the Air Operator POI.

Effective Date: 31 October 2020

PROCESS:

a) An ANCSP should be developed and maintained to protect the usability, reliability, integrity, and safety of the network and data installed on an aircraft and managed by associated ground support systems/equipment.
b) The ANCSP should be sufficiently comprehensive in scope and detailed to accomplish the following:
    1) Ensure that the ANCSP is developed based on the TCH/DAH Aircraft Network Security Guidance (ANSOG/SH) 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 the TCH/DAH manual or a SC 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 and associated ground support systems/equipment, 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 or group of applicable aircraft, an ANCSP document/manual should include the elements listed in Appendix 1.
d) The introduction of the ANCSP 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 ANCSP.
e) The Air Operator should appoint a Data Security Manager by position, who acts as the administrator for the entire ANCSP process with responsibilities listed under Appendix 3.

f) The Air Operator Quality Assurance/Compliance Monitoring Section review the developed ANCSP and confirm that it addresses all applicable requirements in the TCH/DAH network security guidance documents.
g) The Air Operators conducts compliance monitoring of the ANCSP 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 (for instance ROSI).

CONTACTS:
Email: airworthiness@gcaa.gov.ae

APPENDIX 1: ELEMENTS TO BE PART OF THE ANCSP MANUAL

a) Description of the aircraft security network, including the critical areas of the aircraft.
b) Duties and responsibilities for the ANCSP, including persons with authority and responsibility for the safety objective in this alert and the person appointed as Data Security Manager;
c) Qualifications, Training and Experience 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 TCH/DAH specifications. Strict physical and cybersecurity controls should be implemented for the equipment related to the ANCSP. Procedures for reporting lost equipment or equipment that may have been unaccounted for should be in the ANCSP. Additionally, the ANCSP should prohibit the use of personal data storage devices for transferring data intended for an aircraft or system related to the ANCSP. Only operator-approved storage devices should be used to ensure secure transmission;
e) Activities related to the ANCSP 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 used during operations and maintenance activities;
g) Controlling access to Loadable Software Airplane Part (LSAP) librarian resource and to relevant ground support systems;
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) Provisions for tools pooling and tools borrowing;
l) Procedures for part exchanges within its own fleet;
m) CyberSecurity Event recognition and response;
n) CyberSecurity Event evaluation process with considerations for program improvement; and
o) Security Environment Description.

Note: The above list is not exhaustive and may extend the scope of the ANSOG.

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.

Note 1: The above list is not exhaustive and may extend the scope of the ANSOG.
Note 2: The execution of the above tasks may lie with the existing concerned teams.