The First Meeting of Air Traffic Management Automation System Task Force of APANPIRG (ATMAS TF/1)
28 – 30 October 2020

IP/11
A Proactive and Systematic Approach in Protecting Digitised Air Traffic Services Against Cyber Threats in Hong Kong, China

Presented by Hong Kong, China

Introduction

- The Challenge we are facing:
  - Increasing digitisation of air traffic services (ATS) systems
  - Cyber attacks might impact the safety and security of ATS systems

- Objective:
  - Protecting information data, physical assets
  - A systematic approach in implementation of cyber security control measures

Enhanced Controls on Cyber Security

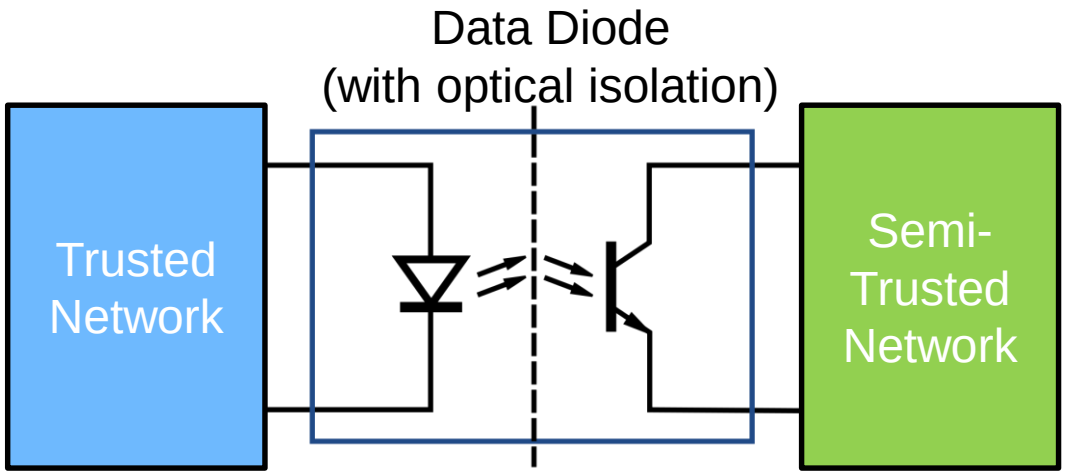
- Documented Policy and Procedure
  - Developed documentation in accordance to ICAO Annex 17 and Doc 9985
  - Provide protection of safety-critical ATS systems against cyber threats
    1. Cyber Security Manual
    2. Cyber Security Handbook
    3. User Account Management Policy for ATS
- Regular meetings to steer the implementation of cyber security control measures throughout the whole life cycle of the ATS systems

Control on Network Infrastructure

- ATS System interconnected for information exchange
- Connection via a common Internet Protocol (IP) data network, Air Traffic Control Data Network (ATCDN)
  - Multi-tier defence-in-depth scheme
  - Network equipment with firewalls, Network Intrusion Detection (NIDS) or Network Prevention System (NIPS) to guard against external connections
  - Data Diode to allow uni-directional communication

Control on Network

- Data Diode Network
  - Restrict uni-directional communication from trusted zone to semi-trusted zone
  - Optical isolation at transmitting and receiving ends
  - Uses for dissemination of surveillance multicast data



Control on User Accounts

- User Account Management
  - Systematic and traceable process for administering user accounts applicable to authorised access to ATS systems
  - Different account privilege for different user groups

Control on System Development

- System Development Life Cycle
  - Having cyber security in mind throughout the system lifecycle
  - Cyber security requirements explicitly laid out in project procedures handbook
  - Include safeguard against cyber threats from an early concept and design stage of a project
  - Conduct Independent Network Security Risk Assessment (INSA)

Controls on Removable Media

- Removable Media Control
  - Common route for importing malicious content to information system
  - Restrict the use of removable media
  - Media are scanned for malicious content by the machine prior to uploading data to ATS systems

Controls on Software Security Patches

- Software Security Patch Management
  - Balance of security with performance
  - Work closely with system manufacturers to evaluate system patch when considered appropriate

Controls on Physical Security

- Physical Security Measures
  - Multi-layer approach
  - From perimeter security down to console/rack level
  - Control measures include:
    - Facility management
    - Security guards
    - CCTV surveillance
    - Room access control
    - Physical lock, etc.

Response to Cyber Security Incidents

- Work closely with Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF)
  - Direct reporting mechanism has established for HKCAD to seek swift assistance from CSTCB
  - Provide advice and independent assessment on cyber security measures implemented
  - Conduct drill exercises to staff awareness and the robustness of the reporting mechanism

Conclusion

- The meeting is invited to:

  a) note the information contained in this paper;

  b) encourage States to strengthen their cyber security management to protect the increasingly digitised ATS against cyber threats; and

  c) discuss any relevant matters as appropriate

Thank you


• Safe • Orderly • Efficient
• Airworthy • Teamwork
Committed to a Safe, Efficient and Sustainable Air Transport System