International Civil Aviation Organization

The Second Meeting of Air Traffic Management Automation System Task Force of APANPIRG (APAC ATMAS TF/2)

Web-conference, 14 – 16 September 2021

Agenda Item 4: ATM Automation System Implementation by States

4.5 Emerging Technology Adaptations and Cybersecurity

PROTECTING AIR TRAFFIC CONTROL SYSTEMS AGAINST CYBER THREATS BY DEPLOYMENT OF DATA DIODE TECHNOLOGY IN HONG KONG, CHINA

(Presented by Hong Kong, China)

SUMMARY

This paper presents the use of data diode technology to safeguard the air traffic control systems from external cyber threats in Hong Kong, China.

1. INTRODUCTION

1.1 Cybersecurity is an increasing challenge faced by aviation industry. The Civil Aviation Department of Hong Kong, China (HKCAD) is committed to the development and implementation of safeguarding measures and controls for continuous protection of the air traffic control (ATC) systems against cybersecurity threats. To protect critical ATC infrastructure against cyber threats, HKCAD has studied and deployed data diode technology in some of our applications, which is different from the conventional approach with the use of firewall, to protect ATC systems. This information paper shares the background and technical details of the data diode deployment for discussion in the meeting.

2. DISCUSSION

2.1 The Three-runway system (3RS) project for the Hong Kong International Airport (HKIA) is under construction and targeted for completion in 2024. To cater for the requirements from stakeholders to support the new runway operation, HKCAD is required to explore an efficient and cost-effective way for disseminating multicast surveillance data from mission-critical ATC systems to other downstream systems, some of which belong to external parties, while protecting the source systems from cyberattacks via the network interface established for those downstream systems.

2.2 Conventionally, serial-based communication is a secure, popular and well-proven way for delivering data at a relatively low data rate. However, it can no longer fulfill the need for distributing data at a high data transmission rate over megabits range. HKCAD has identified a solution based on data diode technology utilizing common LAN protocol. This technology can effectively deliver multicast traffic at sufficiently high data transmission rate while providing an industrially proven solution against cyberattacks, such as malware and infiltration from downstream. The solution

inherently leverages on "law of physics" of the one-way data transmission property, with low operational and maintenance efforts for this type of unique application for civil aviation systems.

2.3 In the current network design in HKCAD, ATC messages are being transmitted back and forth between ATC systems and other downstream systems via HKCAD's External Interface System (EIS), which is a combination of conventional secure routers and firewalls. The multi-tier and zone-based firewalls have been considered an effective and well-proven measure to protect internal systems against cyberattacks from external systems communicating over TCP traffic. However, for multicast traffic concerned, sensitive information including source IP address and multicast group addresses in each data packet, are unavoidably exposed to the downstream systems for multicast traffic due to various limitations in configuring multicast traffic across multi-tier firewalls.

2.4 In pursuit of enhancing the security for multicast data transmission, HKCAD has studied and identified the data diode technology which is widely adopted in various industries, especially when safety-critical industrial processes are involved. For example, this technology is widely deployed in power plants and oil refineries which need to forward operational data from the internal control systems to external parties for real-time monitoring and fault diagnostics. The data diode is also used in commercial aircraft for isolation of flight management systems from passenger inflight entertainment system to prevent malware infiltration from the connected passenger's devices. Similarly, the data diode technology fulfills HKCAD's needs to safely disseminate surveillance data from internal systems to external users while inhibiting malware and zero-day attacks that are originated from external sources.

2.5 The data diode is basically comprised of a transmitting host, an optocoupler, and a receiving host (see Figure 1). In principle, the transmitting host subscribes to the multicast data sources from multiple ATC systems. These data are then encoded with OEM-proprietary protocol within the transmitting host, and transmitted to the receiving host via an optocoupler. The receiving host eventually decodes the data and disseminates them to other downstream systems through LAN connections. The security of data diode technology is benefited by the optocoupler, which is fundamentally a one-way data transmission device such that the data traffic flow direction is solely governed by the law of physics. It is technically impossible to reversely inject any data from downstream to upstream ATC systems, and hence to protect the ATC systems against cyberattacks from downstream system (see Figure 2).

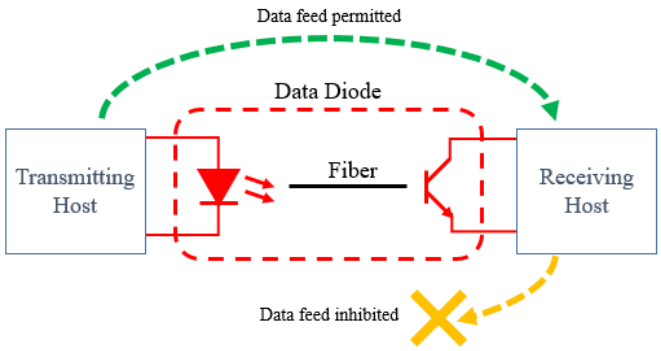

Figure 1: Fundamental structure of unidirectional data diode

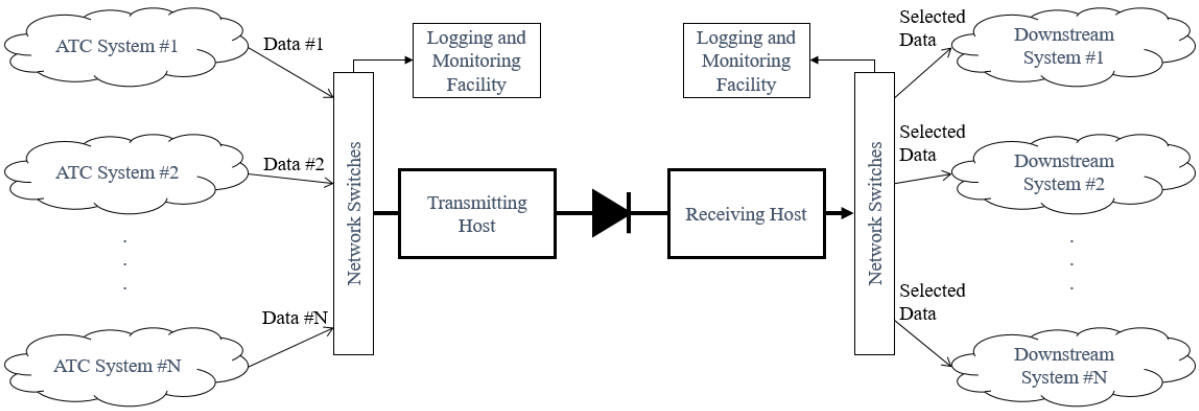

Figure 2: Simplified flow diagram of data diode adopted in HKCAD

2.6 While offering robust protection to the upstream systems, the running cost for maintaining the data diode solution is considered more cost-effective than conventional firewall solution with similar capacity. The data diode solution would not require sophisticated facility for round-the-clock cyber-security monitoring and no expense would be incurred for subscription to any update of cyber security enhancements, currently applied for firewall solutions, to deal with continuous evolution of cyberattacks. Adaptation of data diode to accommodate additional traffic flow is relatively simple and requires less technical knowledge to handle its daily operation.

2.7 After our detailed study and operational trials in using data diode technology for multicast data dissemination, we considered that data diode is a cost-effective and proven technology to enhance cybersecurity for our ATC systems under particular applications. We will continue to explore other potential use cases of data diode to strengthen the overall robustness of our ATC systems against cyber threats.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) encourage States/Administrations to consider and implement cost-effective and proven technologies to safeguard critical ATC systems against cyber threats; and

c) discuss any relevant matters as appropriate.

– – – – – – – – – – – – –