SECURING THE FUTURE OF AVIATION INFORMATION SYSTEMS

A Cyber Security Roadmap for IP-based ACARS communications

WHAT IS ACARS?

Since the 1970s, ACARS (Aircraft Communications Addressing and Reporting System) has provided the means for printed digital transmissions to be exchanged between aircraft and ground stations via radio or satellite.

ACARS console

EMERGING PROBLEM: FINITE RADIO CAPACITY

Projections indicate that radio system infrastructure used to transmit ACARS messages will reach traffic capacity in coming decades. VHF (Very High Frequency) radio, commonly used for ACARS, has a limit as to how much traffic it can accommodate. As global air travel increases in volume, so too does the volume of ACARS transmissions. As ACARS is a requirement across multiple regulatory agencies such as the FAA and EASA for safe and efficient air travel, an inability to transmit ACARS due to lack of traffic capacity would halt the growth of the civil aviation industry worldwide.

THE INDUSTRY SOLUTION: ACARS OVER IP

Aircraft manufacturers, airlines, and regulatory authorities are interested in solving the radio capacity problem by transmitting ACARS messages over IP (Internet Protocol) networks. This solution offers unlimited capacity, answering the need to accommodate growing volumes of ACARS communications.

ACARS OVER IP PRESENTS CYBER SECURITY CHALLENGES

The chief concern among all of the stakeholders in implementation of ACARS over IP is cyber security. Use of IP networks introduces vulnerabilities and attack vectors that are not a factor when using traditional radio systems. Cyber attacks on an IP-based ACARS communication network could lead to valuable data being compromised or lost. As ACARS is linked directly to avionics systems aboard aircraft, a cyber attack could compromise the ability of pilots or air traffic controllers to monitor the status of an aircraft.

THE PATH FORWARD

My project contributes to the efforts of experts across the aviation industry, regulatory organizations, and academia to solve the problem of how to implement ACARS over IP securely. In a research-based white paper format, I draw on technical, regulatory, and business dimensions to recommend the best path forward for implementing ACARS over IP with strong cyber security built in to the program from the beginning.

SUBJECT EXPERTISE

The sponsor for this project is Cyber Business Analytics (CBA), a consulting firm located in Gig Harbor, WA. CBA has deep experience providing cyber security consulting to aviation industry clients, and their subject matter experts have been indispensable providing research guidance and review.

BIG IDEA: SECURITY BY DESIGN

Information projects in organizations of all types typically proceed with a "build it first, secure it later" attitude. With the critical need for the highest standards of safety in aviation, the industry cannot afford to develop ACARS over IP without building strong cyber security into the technology. Further, the ever-changing, increasingly sophisticated cyber attack vectors and threat actors demand that ACARS over IP must be adaptable to respond to cyber risks that don't yet exist.

MAX CARSEN – MSIM 2017

CBA
Cybersecurity and Information
Assurance Solutions

Information School
UNIVERSITY of WASHINGTON