Optimizing Cybersecurity on Today's Connected Military and Commercial Aircraft

Trusted Computing: The COTS Perspective Series

Read About

Protecting Data-at-Rest and Data-in-Motion

Advances in Air Traffic Control

Addressing Airworthiness Security with RTCA DO-326A

Introduction

The number of data communication links and interactions between an aircraft and the ground systems supporting it are ever increasing. If not properly protected, every system, sensor, and module on the aircraft can create a potential vulnerability that can be exploited by unauthorized users to obtain confidential, sensitive data or – worse – disrupt the safe operation of an aircraft. Such threats are of paramount concern for all areas of aviation, including military aircraft and the increasingly top-of-mind UAV market. System developers must safeguard the exchange of tactical information and the integrity of command and control links between ground stations and airborne platforms. Additional security features must be incorporated into avionics systems to minimize the number of different points where an unauthorized user can either input or extract data, also known as the "attack surface."

Ensuring a secure link between aircraft and ground systems is key to protecting sensitive data and minimizing vulnerable points that can be exploited by unauthorized users.

The electronic connectivity onboard commercial or military aircraft includes wireless datalinks for downloading flight recorders or uploading terrain databases and navigation databases. On commercial aircraft, it also includes the networks within the aircraft that support passenger in-flight entertainment and passenger satellite communications (SATCOM) connectivity that enables people to surf the internet while in-flight. Today, it's not uncommon for the aircraft's pilots to use tablet computers in the cockpit. These tablets, known as "electronic flight bags," connect through a Wi-Fi receiver integrated into an Avionics Interface Device in the cockpit. This connects to various avionics data buses, enabling data to be transferred from the avionics systems to the tablet, which the pilot then uses to run applications like calculating take off "V-speeds" and load sheets.

Connectivity means potential targets of opportunity for malicious actors. There may be a computer hacker flying as a passenger, who has the duration of the flight in which to attempt access to the in-flight entertainment system, or more seriously, to the Avionics Interface Device. There may also be a disgruntled airline employee with a valid pass and access to the aircraft and its equipment, who can operate "inside the wire" with no questions asked. The challenge is how to protect avionics against these sorts of vulnerabilities?

Protecting Data-at-Rest

Nearly every aircraft operating in controlled airspace is equipped with a Flight Management System (FMS). This allows flight crews to fly pre-programmed routes from an onboard database containing important information such as airspace structures, ground-based navigational beacons, runway and taxiways. The database also contains the flight trajectories for standard instrument departures (SIDs) and standard arrival routings (STARS) that can fly the airplane automatically after takeoff or during approach.

The FMS is typically updated every 28 days under a procedure known as the Aeronautical Information Regulation and Control (AIRAC) cycle. The database content comes from official state sources by service providers, but the ultimate responsibility of data integrity rests with the end user. FMS database updates are typically uploaded by USB memory stick as a line-maintenance function (the USB content having been downloaded from a secure website or FTP server). This crucial FMS data is stored in non-volatile memory and, if compromised, could prevent an aircraft from operating or landing safely. However, using authentication and encryption techniques, it is possible to guarantee to the end user that the data flow from the FMS service provider to the on-board aeronautical database has not been violated.

Protecting Data-in-Motion

Protecting data-in-motion on the aircraft is equally important. For the networks, there are security layers that provide authentication. Two key examples of these security layers are the security protocol suites Internet Protocol Security (IPsec) and MAC Security standard (MACsec: IEEE 802.1AE). They can be built into the network layers to ensure that end-to-end communication cannot be disrupted, hacked, or tapped into. The MACsec standard strengthens network security by identifying unauthorized local area network (LAN) connections and excluding them from communication within the network. The protocol authenticates nodes through a secure exchange of randomly generated keys, ensuring data can only be transmitted and received by MACsec-configured nodes, and provides optional point-to-point, Layer 2 encryption between devices on a virtual or physical LAN. IPSec provides similar protection for a wide area network (WAN). It works on IP packets at Layer 3 (as opposed to Ethernet frames at Layer 2, like MACsec). For an FMS, which traditionally required data to be uploaded manually, but can now receive such uploads via wireless technology, such protocols are important for protecting the integrity of the data during transfer.

Security and Next Generation Air Traffic Control

In addition to the connected aircraft itself, with the Next Generation Air Transportation System (NextGen) in the US and Single European Sky ATM Research (SESAR) in Europe, advanced air traffic control systems are quickly coming online to enable denser air traffic with reduced tolerance for error.

A surveillance technology that uses GPS satellite navigation data to determine an aircraft's position, called Automatic Dependent Surveillance-Broadcast (ADS-B), will be mandated in many controlled airspace regions from 2020. ADS-B will send out automatic position report pulses, called extended squitters, to broadcast the aircraft's position. This information can be received by ATC ground stations as a replacement for secondary surveillance radar, since no interrogation signal is needed from the ground.

ADS-B can also be received by other aircraft to provide situational awareness and allow self-separation. On more advanced aircraft, it will be used to report not just the aircraft's current position but also its flightpath to destination so that the ATC system and other aircraft can also predict where the aircraft will be in the future. This predictive data enables other aircraft in the same area to compute their own route to ensure that they don't converge with the first aircraft's flight path. The Search Acquisition Radars used at airports for years are rapidly going away because they are only good for providing line-of-sight data. With today's sophisticated onboard navigation systems, it's now better to let the aircraft work out amongst themselves how closely they can safely approach each other in the sky.

The DO-326A Airworthiness Security Process Specification

To provide guidance for handling the threat of intentional, malicious interference with aircraft systems, the Radio Technical Commission for Aeronautics (RTCA) released DO-326A, titled "Airworthiness Security Process Specification." This document complements other advisory material, such as the hardware and software safety certification guidance documents DO-254 and DO-178C. DO-326A outlines compliance objectives and data requirements for aircraft and airborne equipment manufacturers.

DO-326A provides guidance on the interactions between security and safety. As the DO-254 safety certifiability standard for hardware requires a Plan for Hardware Aspects of Certification (PHAC), and DO-178C requires a Plan for Software Aspects of Certification (PSAC), the DO-326A standard calls for a Plan for Security Aspects of Certification (PSecAC). Today, any new aircraft system that is connected to the outside world will have to address the DO-326A requirements that are flowing down from the regulators.

DO-326A covers such things as navigation databases and terrain awareness warning databases, though it doesn't provide specific direction on how to implement required safeguards. Instead, it mandates a process under which all threat scenarios and use cases are identified and adequate measures are put in place to mitigate them. Under DO-326A a system integrator deploying any new avionics, such as a navigation system, onto an aircraft must demonstrate that they have protection measures in place and that they've identified the necessary aircraft and security perimeters to mitigate against a malicious actor.

In recent years, as FAA and EASA regulators are being asked more about cybersecurity, there has been a growing emphasis and insistence that DO-326A processes are put into action. That makes it incumbent on avionics system integrators to educate themselves so that they are aware of this standard, as it will only become more important in coming years.

Author(s)

Paul Hart
Chief Technology Officer
Curtiss-Wright Defense Solutions

Conclusion

Implementing the right security strategy and features is of paramount importance to protect the exchange of tactical information, maintain the integrity of command and control links between ground stations and airborne platforms, and minimize the number of different points where an unauthorized user can either input or extract data. For more information about Trusted Computing mechanisms and aircraft certification protocols, explore the Learn More section below.

Learn More

Curtiss-Wright Products

- Curtiss-Wright TrustedCOTS™
- DO-254 & DO-178 Safety-Certifiable COTS Solutions
- DO-254 Single Board Computers
- DO-254 Graphics and Video modules
- Data-at-Rest Encryption

Curtiss-Wright Blog

- Enhancing Network Security with MACsec (IEEE 802.1AE)

Curtiss-Wright White Papers

- Accelerate Time-To-Market With Safety-Certifiable Airborne Electronics Hardware
- Understanding Your Safety-Certifiable COTS Options: A Closer Look at the Subsystem Level
- Why Dissimilar Redundant Architectures Are a Necessity for DAL A
- Is Arm the Future for Airborne Platforms in Military and Aerospace?
- Optimal Multicore Processing for Safety-Critical Applications
- Enabling Multi-Core Processing in DO-254/178 Safety-Certifiable Avionics
- Trusted Computing: The COTS Perspective Series
  1. Introduction to COTS-based Trusted Computing
  2. Trusted Boot
  3. Hardware Features for Maintaining Security During Operation
  4. Considering the Role of Hardware in Securing OS and Hypervisor Operation
  5. Application Development, Testing, and Analysis for Optimal Security
  6. Developing a Secure COTS-Based Trusted Computing System
  7. The Impact of Protecting I/O Interfaces on System Performance
  8. Decomposing System Security Requirements
  9. Establishing a Trusted Supply Chain
  10. Certification Authorities for Trusted Computing in Military and Avionics Products
  11. International Certification Authorities for Trusted Computing
  12. Optimizing Cybersecurity on Today's Connected Aircraft