DO-326A Cybersecurity for aerospace embedded software

The problem

An aircraft interacts with countless different networks and systems around the globe. The possible threats to aircraft operations are numerous and include: Spoofing, Exploiting, Denial of Service and Counterfeiting[1]. As an example, the U.S. Air Force in a recent workshop has identified risks to Communications, Navigation and Flight Instrument, Flight Control, Collision Avoidance, Health and Monitoring amongst other systems that are vulnerable to these different threats[2].

With the advent of access to higher bandwidth, advanced wireless and cellular (3G/4G) connectivity, ensuring the safety and security of aircraft avionic systems (where you can find the flights controls, the flight management and navigation), the aircraft information systems and the in-flight entertainment systems, among other systems is critical.

To address these concerns, DO-326A was developed to handle the threat of intentional unauthorized electronic interaction to aircraft safety. This standard defines the activities that need to be performed in support of the airworthiness process. These activities include but are not limited to the Security Scope Definition, the Security Risk assessment and security development. This standard is used conjointly with its companion document DO-355 to address airworthiness security for continued airworthiness.

Our offering

CS Canada owns the know how to perform the complete security assessment and security process implementation of your safety critical system through the application of DO-326A.

- Perform aircraft or system level security risk assessment activities
    - Identify the System Security Scope
        - Assets, security perimeter, security environment
    - Perform the preliminary security risk assessment
        - Threat scenarios and threat conditions
    - Perform the System Security Risk Assessment

[1] 2013 Honeywell Presentation: Civil Aviation and Cybersecurity
[2] 2017 U.S. Air Force workshop: Managing Cybersecurity Risks

1 (866) 748-8258
info@cscanada.ca
www.cscanada.ca

Montreal, Qc, Canada
East Hartford, CT, USA

- Provide training services for Airworthiness Cybersecurity Engineering
    - Learn how cyber-security threats can increase the risk associated with known safety-related hazards
    - Become familiar with security focused RTCA guidance documents including DO-326A, DO-356 and DO-355
    - Learn about specialized techniques to support risk assessment activities
    - Develop an understanding of how to produce documentation that will meet the certification expectations
    - Gain an insight of expected changes in upcoming DO-356A

Benefits

Our customers within the aerospace industry can implement DO-326A rapidly and efficiently, thanks to our support, and therefore ensure that their systems will be safe, and that people's life within and around planes will be safeguarded.

Why CS Canada?

In order to meet these cybersecurity challenges, CS Canada has assembled a highly skilled team with substantial experience in critical real-time software development and V&V.

1 (866) 748-8258
info@cscanada.ca
www.cscanada.ca

Montreal, Qc, Canada
East Hartford, CT, USA