Industry Brief: Aerospace and Avionics

MŌCANA

Stabilizer Trim Controller

Weather Systems Controllers

Navigation Controller

Leading Edge Slat Drive Controllers

Inbound Attacks

Infotainment Systems

Communication Controllers

Trailing Edge Flap Drive Controllers

Physical Attacks

Engine-Driven Pump Controllers

Collision-Avoidance Systems

Replay Attacks

Radar and Sonar Controllers

Aircraft and Defense Systems Present Many Surfaces for Attack

Ensuring Safety, Reliability and Compliance

Cyber threats have moved from cyber attacks to cyber warfare. Aircraft flight control system, monitoring, commercial and military communication, navigation, weather, collision-avoidance systems, radar, sonar, and major weapons systems may be vulnerable due to a lack of strong embedded cryptographic controls, including: multi-factor authentication, secure boot, secure update, and secure, encrypted communications.

Aerospace and avionics manufacturers must ensure compliance with cybersecurity standards such as NIST 800-53, Revision 4, IEC 62443-3-3, FIPS 140-2, and DO-178. Keeping up with these standards as well as emerging standards from the Industrial Internet Consortium (IIC) and Industrie 4.0 is challenging. New regulations such as GDPR in Europe raise the stakes for non-compliance to more than €20 million per incident. Older protocols such as Modbus, DNP3 and BacNet can be difficult to secure.

For commercial and military missions, risk can be measured in terms of safety and reliability of the systems. While data privacy is important, ensuring physical human safety and success of the mission success is absolutely critical.

Mocana's Proven Cybersecurity Solution

Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications by giving industrial automation manufacturers, OEMs and critical infrastructure operators an easy way to:

- Harden avionics controllers, communications, navigation, collision-avoidance, and weapon systems with multi-factor authentication using X.509 certificates and trust chaining
- Secure the boot process to validate the firmware, OS and applications
- Enable secure, cryptographically-signed over-the-air (OTA) and over-the-web (OTW) firmware updates
- Integrate hardware or software-based roots of trust such as TPM, SGX, TrustZone, HSMs, SIMs, and MIMs
- Replace open source crypto software such as OpenSSL.

For more information on Mocana's comprehensive IoT Security Platform and how it can help you secure your critical infrastructure, visit our website at mocana.com or send us an email via sales@mocana.com.