EASA Aviation Cyber Security Overview

Sofema Aviation Services (SAS) www.sassofia.com considers fundamental issues related to the challenge to address cyber security threats within EASA regulated Organisation

Introduction

The EASA Cyber Security Framework provides a structured approach to managing cyber risks, ensuring dependability and trustworthiness across aviation systems. Overcoming challenges—like defining common risk acceptability—requires collaboration, the adoption of best practices, and continuous improvement.

By aligning safety and cyber security processes, organizations can achieve a balanced approach that maintains compliance while safeguarding aviation systems against emerging cyber threats.

- As the aviation industry grows increasingly digital and interconnected, cyber security is paramount to maintaining operational continuity, passenger safety, and regulatory compliance.

EASA Cyber Security Framework

The EASA Cyber Security Framework ensures that organizations operating within the European aviation sector meet specific regulatory and operational requirements to mitigate cyber security risks. These guidelines stem from:

Regulation (EU) 2019/947 and 2019/945 for drones.

EASA NPA 2019-01 introducing cyber security in aviation safety management systems.

AMC 20-42 (Cyber Security for Safety) provides acceptable means of compliance for addressing cyber risks.

The framework emphasizes cyber resilience, aligning with broader international initiatives like ICAO's Aviation Cyber Security Strategy and promoting a risk-based approach.

Key Challenges in Agreeing on Common Risk Acceptability

Agreeing on common risk acceptability involves achieving consensus on what levels of cyber risk are tolerable and manageable across stakeholders. Challenges include:

a. Lack of Uniform Standards

- Variations in how different stakeholders (OEMs, airlines, maintenance organizations, ANSPs, etc.) interpret cyber risk.

- Lack of alignment between operational (safety) and IT (cyber security) perspectives.

b. Complex Interdependencies

- Aviation systems involve numerous interconnected components: hardware, software, cloud-based systems, and third-party services.
- A single vulnerability in one area can propagate across the ecosystem, creating difficulty in assessing cumulative risk acceptability.

c. Rapid Technological Changes

- Emerging technologies (IoT, AI, big data) outpace the regulatory framework and standards.
- Adapting to evolving cyber threats while maintaining compliance can be slow.

d. Balancing Safety vs. Cyber Security

- Prioritizing cyber security alongside aviation safety can be complex, as adding cyber safeguards may impact safety-critical systems' performance or reliability.

e. Risk Communication

- Ensuring effective communication and shared understanding of risks among multi-disciplinary teams (engineers, IT security specialists, safety managers, and executives).

f. Resource and Knowledge Gaps

- Limited cyber security expertise within some organizations.
- Small or medium-sized organizations may lack the resources to implement comprehensive cyber security risk management strategies.

3. Best Practices to Support Dependability and Trustworthiness

To overcome the challenges, organizations can implement the following best practices:

a. Adopt a Risk-Based Approach

- Use risk-based methodologies to assess the probability and impact of cyber risks. Example frameworks include:
  - ISO/IEC 27005: Risk Management in Information Security.
  - NIST Cyber Security Framework: Identify, Protect, Detect, Respond, Recover.
  - DO-326A/ED-202A: Airworthiness Security Process Specification.

b. Define Common Risk Acceptability Criteria

- Stakeholders must collaborate to agree on common Risk Acceptability Levels (RALs) based on safety, security, and business impact.
  - Develop Quantitative Risk Matrices to clearly define thresholds for "acceptable," "tolerable," and "unacceptable" risks.

- Incorporate these into Cyber Security Management Systems (CSMS).

c. Embed Cyber Security into Safety Management Systems (SMS)

- Integrate cyber security into existing SMS processes to assess and mitigate risks alongside safety risks:
  - Hazard Identification: Identify cyber security hazards impacting safety.
  - Risk Assessment: Determine the likelihood and severity of cyber-related failures.
  - Risk Mitigation: Deploy safeguards to maintain the safety and integrity of systems.

d. Promote Threat Intelligence Sharing

- Collaborate with Information Sharing and Analysis Centers (ISACs) and regulatory bodies to share cyber threats, vulnerabilities, and mitigation strategies.

e. Conduct Regular Cyber Security Audits

- Perform vulnerability assessments and penetration testing to evaluate system resilience against cyber attacks.
- EASA-compliant audits ensure continuous monitoring and alignment with regulations.

f. Build Cyber Resilience into System Design

- Integrate cyber security measures during the design phase of systems (Security by Design).
- Implement Defense-in-Depth strategies:
  - Multi-layered security controls (e.g., firewalls, encryption, multi-factor authentication).
  - Isolation of critical systems to prevent lateral movement during attacks.

g. Implement Cyber Incident Response Plans (CIRP)

- Develop and test response plans to address cyber security incidents.
- Ensure timely reporting to regulatory authorities and stakeholders, as required by EASA.

h. Enhance Training and Awareness

- Conduct cyber security training for engineers, managers, and frontline employees.
- Promote a security culture that encourages reporting of potential cyber threats or vulnerabilities.

i. Leverage Third-Party Expertise

- Collaborate with cyber security specialists and trusted third-party auditors to assess and enhance cyber defenses.

j. Continuous Monitoring and Threat Detection

- Utilize Security Operations Centers (SOCs) and automated threat detection tools to continuously monitor systems and detect anomalies.

Steps for Implementation

1. Risk Identification and Assessment: Map out systems and processes, identifying assets and associated cyber risks.
2. Develop Acceptability Criteria: Align risk thresholds and mitigation strategies across the supply chain.
3. Mitigate Risks: Deploy technical, procedural, and operational safeguards.
4. Monitor and Respond: Use real-time monitoring and defined response plans to address incidents.
5. Iterate and Improve: Continuously evaluate the framework to address emerging threats and regulatory updates.

See the following 2 day course https://sassofia.com/course/implementing-information-cyber-security-program-easa-part-145-organization-2-days/ for comments or questions please email team@sassofia.com