Software & Airborne Electronic Hardware Standardization Conference

Electronic Flight Bag (EFB) & Security

Presented by: Peter Skaves, AIR-130, Avionic Systems Branch
Briefing Objectives

- Acronyms
- Risk Management Guide for IT Systems
  - NIST Special Publication 800-30
- Aircraft Certification Approval Process
  - System Safety Development Process
- Future EFB Policy & Direction
  - EFB System Risk Assessment
  - EFB “Gateway” System Function
  - EFB Classes and Approval Process
  - EFB Type “A” & “B” Software Applications
- Discussion and wrap-up
Acronyms

✓ Acceptable Means of Compliance (AMC)
✓ Advisory Circular (AC)
✓ Aircraft Certification Service (AIR)
✓ Airline Administrative Communication (AAC)
✓ Electronic Flight Bag (EFB)
✓ European Aviation Safety Agency (EASA)
✓ Federal Information Processing Standards (FIPS)
✓ Flight Standards Service (AFS)
✓ Information Technology (IT)
✓ Internet Protocol (IP)
✓ National Institute of Standards and Technology (NIST)
✓ Principal Inspector (PI)
✓ System Development Life Cycle (SDLC)
✓ Special Publication (SP)
✓ Technical Standard Order (TSO)
✓ Temporary Guidance Leaflet (TGL)
SP 800-30 Security Risk Management

- Risk Management Encompasses Three Processes
  - Risk Assessment
  - Risk Mitigation
  - Evaluation and Assessment

- Risk management is the process that allows Managers to balance the economic costs of protective measures to ensure the system works correctly and is not adversely impacted

- This process is not unique to the Information Technology (IT) process
System Development Life Cycle

- Integration of Risk Management into the System Development Life Cycle (SDLC)
- SDLC Phases
  - Phase 1 – Initiation
  - Phase 2 – Development or Acquisition
  - Phase 3 – Implementation
  - Phase 4 – Operation or Maintenance
  - Phase 5 – Disposal
Phase 1 – Initiation

- The need for the IT system is expressed and the purpose and the scope of the IT system is documented

- Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations strategy
Phase 2 – Development or Acquisition

- The IT system is designed, purchased, programmed, developed, or otherwise constructed.
- The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development.
Phase 3 – Implementation

- The system security features should be configured, enabled, tested, and verified.

- The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation.
Phase 4 – Operation or Maintenance

- The system performs its functions. Typically, the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.

- Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational production environment (e.g., new system interfaces).
Phase 5 – Disposal

- The phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software.

- Risk management activities are performed for system components that will be disposed or replaced to ensure that the hardware and software are properly disposed of.
Risk Assessment

- Risk assessment is used to determine the extent of the potential threat and risk associated with an IT system throughout its SDLC.

- Risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

1) System Characterization
2) Threat Identification
3) Vulnerability Identification
4) Control Analysis
5) Likelihood Determination
6) Impact Analysis
7) Risk Determination
8) Control Recommendations
9) Results Documentation
List of Current and Planned Controls

Step 4.  Control Analysis

Threat Statement

List of Potential Vulnerabilities

List of Current and Planned Controls
Step 5. Likelihood Determination

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Step 7. Risk Determination

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 8. Control Recommendations

Step 9. Results Documentation
(1) System Characterization

The organization that conducts the risk assessment must first collect system-related information, which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System Mission
- System and data Criticality
- System and Data Sensitivity
(2) **Threat Identification**

- A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability.

- A vulnerability is a weakness that can be accidentally triggered intentionally or exploited.

- A threat-source does not present a risk when there is no vulnerability that can be exercised.

- In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls.
If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization’s security policies, planned security procedures, and system requirements definition.

If the IT system is being implemented, the identification of vulnerabilities should include planned security features described in the security design documentation and the results of system certification test and evaluation.

If the IT system is operational, the process of identifying the vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.
(3) Vulnerability Identification
(sheet 2 of 2)

Penetration Testing

✓ A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, known as a Hacker.

✓ Penetration testing may be conducted in several ways.

✓ The most common difference in penetration testing is the amount of knowledge the Hacker has of the system being tested.

✓ Some Hackers have complete knowledge of the infrastructure to be tested, often including network diagrams, source code, and Internet Protocol (IP) addressing information.
(4) **Control analysis** (sheet 1 of 2)

- Security controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software).

- Control Categories may be classified as preventive or detective
  
  - Preventive controls inhibit attempts to violate security and include encryption and authentication
  
  - Detective controls warn of violations or attempts to breach security and include audit trails, intrusion detection methods, and checksums
(4) **Control analysis** *(sheet 2 of 2)*

- **Preventive Technical Controls**
  - Authentication
  - Authorization
  - Access Control Enforcement
  - Protected Communications

- **Detection & Recovery Technical controls**
  - Audit
  - Intrusion Detection and Containment
  - Proof of Wholeness
  - Restore Secure State
  - Virus Detection and Eradication
(5) Likelihood Determination

- **Likelihood Level**

  1) **HIGH** - The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective

  2) **MEDIUM** – The threat source is motivated and capable, but controls are in place that may impede successful exercise and vulnerability

  3) **LOW** – The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised
(6) Impact Analysis

The major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability

- Loss of Integrity – Unauthorized changes are made to the data or IT system by either intentional or accidental acts
- Loss of Availability – If a mission-critical IT system is unavailable to its end users, the organization’s mission may be affected
- Loss of Confidentiality – System and data confidentiality refers to the protection of information from unauthorized disclosure (e.g., personal aircraft flight crew or passenger information)
(7) Risk Determination

- The Risk Determination methodology described in SP 800-30 does not directly map to the Aircraft Certification System Safety Assessment (SSA) Process
  - SP 800-30 describes a process to assign threat likelihood levels and impact levels
  - The threat likelihood level is then multiplied by the Impact level to derive a risk level
- RTCA SC-216 “Aeronautical System Security” is the best forum to address Risk Determination mapping to aircraft operations
(8) **Control Recommendations**

- The goal of the control recommendations is to reduce the level of risk to the IT system and its data to an acceptable level.
- The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:
  - Effectiveness of recommended options
  - Operational Impact
  - Safety and Reliability
  - Legislation and Regulation
  - Organizational policy
(9) **Results Documentation**

- Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

- A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.
We have just finished a high level overview of the Risk Management Guide for Information Technology Systems.

We will now review a high level Aircraft Certification Service System Safety Process.

In order to address Safety & Interoperability between the aircraft and infrastructure, the two different processes must be evaluated and any gaps or inconsistencies identified and addressed.
SP 800-30 Vs. ARP 4754

Harmonization Issues

1) Some SC-216 Team members believe that SP 800-30 and ARP 4754 are two separate processes that cannot be combined and that each process must be conducted independently.

2) Some SC-216 members believe that SP 800-30 was written for ground base IT systems and is not applicable to aircraft avionics.

3) Some SC-216 members believe that SP 800-30 and ARP 4754 are interwoven processes and gaps and differences should be identified and mitigated.
<table>
<thead>
<tr>
<th>System Certification Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Plan</td>
<td>4.4.1</td>
</tr>
<tr>
<td>Development Plan</td>
<td>4.4.3</td>
</tr>
<tr>
<td>Architecture and Design</td>
<td>4.4.4</td>
</tr>
<tr>
<td>Requirements</td>
<td>5.2 and 5.3</td>
</tr>
<tr>
<td>Validation Plan</td>
<td>7.7.1</td>
</tr>
<tr>
<td>Verification Plan</td>
<td>8.5.1</td>
</tr>
<tr>
<td>Configuration Management Plan</td>
<td>9.0</td>
</tr>
<tr>
<td>Process Assurance Plan</td>
<td>10.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Index</th>
<th>4.4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Hazard Assessment</td>
<td>6.1</td>
</tr>
<tr>
<td>Preliminary System Safety Assessment</td>
<td>6.2</td>
</tr>
<tr>
<td>System Safety Assessment</td>
<td>6.3</td>
</tr>
<tr>
<td>Common Cause Analysis</td>
<td>6.4</td>
</tr>
<tr>
<td>Validation Data</td>
<td>7.7</td>
</tr>
<tr>
<td>Verification Data</td>
<td>8.5</td>
</tr>
<tr>
<td>Evidence of Configuration Management</td>
<td>9.2</td>
</tr>
<tr>
<td>Evidence of Process Assurance</td>
<td>10.4</td>
</tr>
<tr>
<td>Certification Summary</td>
<td>4.3</td>
</tr>
</tbody>
</table>

**NOTE:** Shading indicates minimum certification data.
Certification Considerations for Highly Integrated or Complex Aircraft Systems

Describes the Aircraft Systems Engineering Process

- Requirements Capture
- Allocation of Requirements
- Architectural Considerations
- Software Design Assurance Level Determination
- Hardware Level Assurance Level Determination
- Integration
ARP 4754 (sheet 2 of 2)

- **Safety Assessment Process (high level)**
  - ✓ Functional Hazard Assessment (FHA)
  - ✓ Preliminary System Safety Assessment
  - ✓ System Safety Assessment

- **Requirements Validation**

- **System Verification**
Intended Aircraft Function

System Development Processes
(ARP 4754)

Function, Failure & Safety Information

System Design

Implementation

Software Development Life-Cycle
(DO-178B)

Hardware Development Life-Cycle
(DO-254)

Aircraft System Development Process

Functions & Requirements

Software Life-Cycle Process

Hardware Life-Cycle Process

Safety Assessment Process Guidelines & Methods
(ARP 4761)
What is EFB Security Policy Today?

- Future directions on EFB security
  - The FAA currently does not have specific policy and guidance for EFB system security
  - EFB manufacturers and operators determine security implementations on a case-by-case basis
  - What are the risks associated with EFB system and security?
  - What is the regulatory basis for EFB security?
  - Should the FAA develop specific policy and guidance for EFB systems or have general policy?
Possible EFB System Risk Assessment

- Risk assessment is used to determine the extent of the potential threat and risk associated with an EFB system throughout its SDLC.

- Risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability, and the impact of that adverse event on the EFB system and aircraft operation.

1) System Characterization
2) Threat Identification
3) Vulnerability Identification
4) Control Analysis
5) Likelihood Determination
6) Impact Analysis
7) Risk Determination
8) Control Recommendations
9) Results Documentation
EFB “Gateway” System Functions

- EFB may be used for data communications between the aircraft and the National Airspace System (NAS)
- Primary use for Airline Administrative Communications (AAC)
- Possible to exchange large volumes of information between aircraft and airline operations centers
- Possible to eliminate millions of paper copies
Typical Application & Services

Wireless Cabin Distribution

Attendant EFB

Cockpit Terminal - EFB

Airborne Communication Links (ACARS, XM, Sirius, JetConnect)

Server

Air to Air Data Link (Sirius/XM or JetConnect)

Typical Applications and Services

Flight Ops
- Weather
- Electronic Manuals/Charts
- Cabin Surveillance
- Surface Moving Maps
- Flight Papers/Data

Onboard/Passenger
- Rebooking/IRROPS
- Customer Profiles
- Buy On Board
- Live Audio
- Email/WAP Browsing

Maintenance
- *FIX
- Flight Data Downloads
- Electronic Logbook
- Maintenance Data Collection
- Electronic MEL
EFB Data Connectivity

Ethernet router is a “certified” firewall that allows access to internal aircraft avionics and external aircraft interfaces.
Possible Architecture & Infrastructure
EFB Classes and Approval Process

**Portable Equipment**
- **Class 1**
  - Portable
  - Usable above 10,000 ft. and Airport surface
  - Limited by AC 120-76A

- **Class 2**
  - Portable devices
  - Crashworthy-mounted
  - EMI approval required
  - All phases of flight
  - Ships power
  - Read only airplane data
  - Video interface
  - Limited by AC 120-76A

- **Class 3**
  - Installed
  - Ships power
  - All flight phases
  - Datalink
  - Interactive Apps
  - Video interface
  - Increased Functionality

**Installed Equipment**
- **Type A & B Applications**
- **Certified applications**
- **Operations approval**
EFB & Flight Deck Integration
Type “A” Software Applications

- Type “A” software application criteria
  - May be hosted on Class 1, 2 & 3 EFB Systems
  - Requires Flight Standards District Office (FSDO) / PI Approval
  - Does not require AIR design approval

- Type “A” software application examples
  - Flight Operations Manuals (FOMs)
  - Company Standard Operating Procedures (SOPs)
  - Aircraft Flight Log and Servicing Records
  - Airplane Flight Manuals and Supplements
  - Aircraft Performance Data
  - Aeronautical Information Manual (AIM)
Type “B” Software Applications

Type “B” software application criteria
- May be hosted on Class 1, 2 & 3 EFB Systems
- Requires an PI / AEG Evaluation Does not require AIR design approval

Type “B” software application examples
- Performance calculations (e.g., Takeoff, en route, approach and landing, missed approach)
- Moving Map(s) without own ship position
- Runway limiting performance calculations
- Panning, zooming, scrolling and rotation of approach charts
- Weather and aeronautical data
- Cabin-mounted video surveillance
Boeing Class 3 Installed EFB

Type “B”
Type “C”
Type “B”

Type “A”
Type “B”
Type “A”
ARINC eFlight Deck Airborne Solution

Basic ACARS
Security Sensors
QAR
GateLink
Airborne Video
Printer

Electronic Flight Bags & Security
Electronic-Logbook
Aeronautical Charts – Access Methodology
This Special committee is needed to form a consensus and document guidance for a network security assurance process and acceptable means of compliance for safe, secure and efficient airspace operations.
Questions

Peter Skaves, Aircraft Certification Service

Peter.Skaves@faa.gov

(425) 802-0395