Security Assessment of the Aircraft Architecture

Prepared By**: Shail Patel**

v 1.0 October | 19 | 2023

Table of Contents

Executive Summary

An architectural security risk assessment was performed on the given commercial aircraft to identify practical attack scenarios and to qualify their potential safety-impacts and likelihoods.

During this process, it was observed that there was no indication that adding more complexity would increase security. More specifically, the use of attacker characteristics is independent of the security of the system.

This report describes the methodology leveraged to perform the risk assessment, the initial assumptions & the security environment, identification of critical systems in the aircraft, attack vectors, assessments of risks with proposed mitigations, proposed security changes in the architecture and verification cases.

Approach:

For the purpose of this exercise, the security risk assessment methodology used is based upon the Airworthiness Security Process Specification (DO-326A) and focused on security scope definition and security risk assessment. This architectural assessment aims to identify and analyze all potential security threats introduced by design and interfacing stakeholders. In addition to identifying security threats, the assessment seeks to qualify the potential safety impact to the aircraft as a measure of attack difficulty and likelihood of threat realization according to the industry standard RTCA Airworthiness guidelines. A likelihood metric is introduced as a qualitative measure to estimate the probability that a threat scenario will occur. The objective is to proactively evaluate and identify those security risks that may cause potential safety risks. This report specifically leverages the DO-356 method of using threat trees for evaluating security risks.

This assessment is performed at an architectural level to identify high-level systemic vulnerabilities as opposed to specific vulnerabilities of limited breath: the analysis aims to explore system level security risks, and not flaws specific to an individual software or hardware implementation. While it is important to consider such flaws in an overall security process, the purpose of this exercise is to qualify practical risk scenarios stemming from expanding aircraft connectivity and current system architectures.

Following DO-326A, I begin with the security scope definition. This step included identifying the subject, the interfaces external to the subject, the actors that interact with the subject over these interfaces, and the functions that the subject performs. After this step, I limited the scope of the assessment to threats that could affect the airworthiness of the aircraft by identifying threats for the major flight critical systems in the provided architecture. Attack trees were then utilized to characterize each of the representative threats in a formal and methodical approach. Using the attack trees and representative attacker characteristics, the attack trees were analyzed to determine the minimum attack paths. Combining the threat likelihood and impact, a risk assessment was generated for each aircraft threat and relevant security measures were proposed in the architecture.

Initial Assumptions and Security Environment:

The review of the Security Environment requires that the relevant "domains" are identified based on the given architecture (e.g., on-board, ground, and air-ground communications). For the purpose of analysis, the given architecture in this exercise recognizes trustworthiness of the elements as binary, where an entity is either considered "trustworthy" or "not trustworthy" in contrast to the approach described in RTCA DO-356 where the approach considers trustworthiness of the threat source with different possible levels according to the severity of misuse of the asset under assessment (e.g., the highest trustworthiness level is assigned to an entity using and managing assets of catastrophic safety impact).

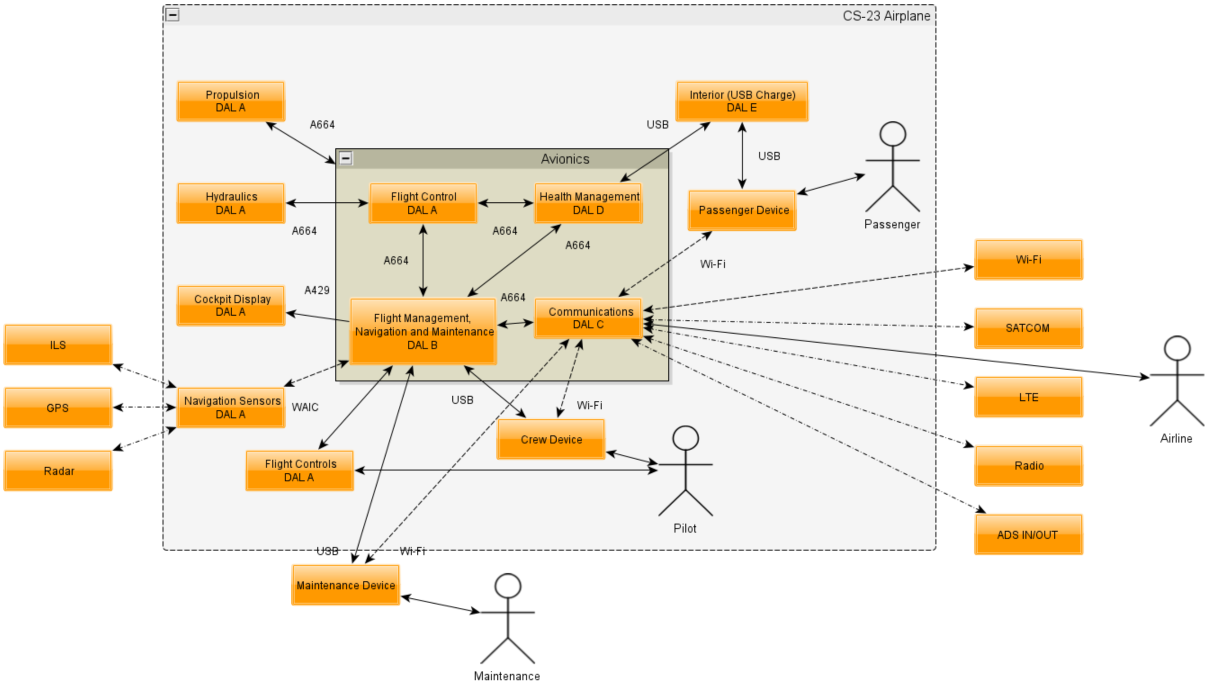
For the given architecture, the tables below illustrates initial assumptions to support the binary determination of trustworthiness as part of the security environment review.

Assumptions about External Entities	***Trusted***	***Non-Trusted***
	- Aircraft System Suppliers - Air Navigation Service Providers	- Passengers - Airline - Maintenance

Assumptions about External Interfaces	***Trusted***	***Non-Trusted***
	- Plugs, connectors, cables, and any piece of equipment (even in the cabin) that are not readily accessible to unauthorized persons (i.e., located behind structure/interior panels that requiring tampering of aircraft parts)	- E-tools and media (e.g., USB mass storage devices, maintenance equipment, Electronic Flight Bag (EFB), passenger devices)

Assumptions about Data Communications	***Trusted***	***Non-Trusted***
	- ADS-B, RADIO, SATCOM	- Wi-Fi, LTE, ILS, GPS, RADAR

Assessment:



Critical Systems: As per CS 23.2500(b) focus on intentional unauthorized electronic interaction (IUEI), for the purpose of this assessment, I evaluated the aircraft's avionics architecture as it is one of the most critical systems due to their criticality for safe flight operations. The major components include Flight Control, Flight Management, Navigation & Maintenance, Avionic Busses, and Communications which are available to the flight crew and maintenance crew.

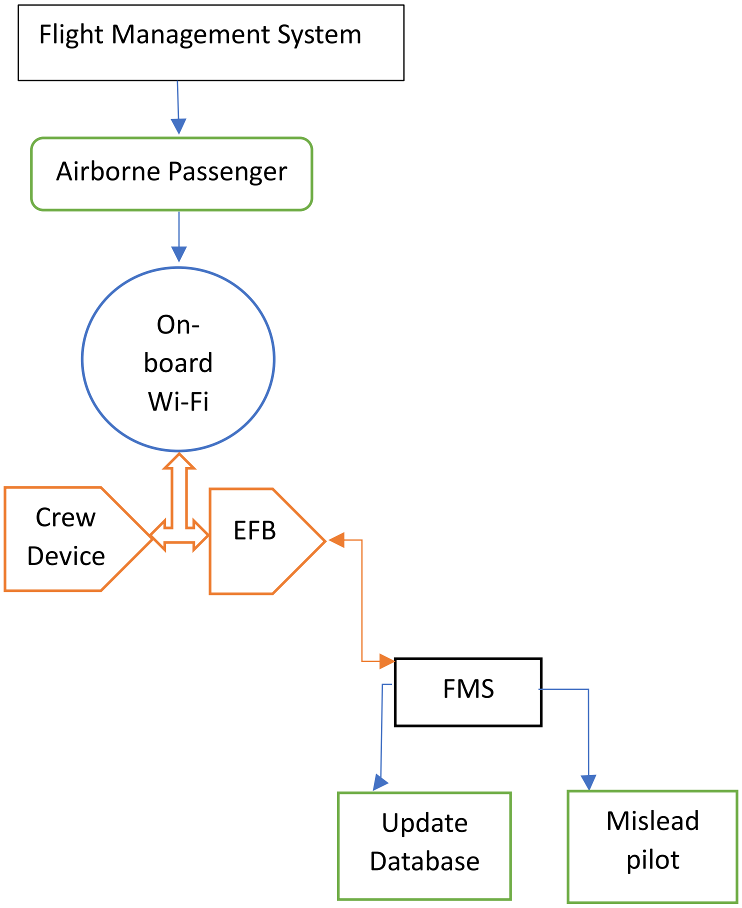
The assessment scope considers an attack surface to be defined by any available means of providing a digital input to the aircraft including USB, Wi-Fi, etc. I considered only those avionics internal to this aircraft as part of the risk analysis; security of the ground systems and networks are not considered.

Attack Scenarios & Attack Trees:-

1. *Flight Management System(FMS)*

   In this scenario, the goal of an attacker is to compromise the FMS. The FMS is responsible for managing the flight plan and the navigation database. FMS functions include determining the course to the next waypoint and identifying the current position and the surrounding environment.
   Due to the tightly integrated nature of this avionics architecture and lack of physical and logical segmentations, a malicious passenger uses the common onboard duplex Wi-Fi from their device (tablet or laptop) to obtain unauthorized

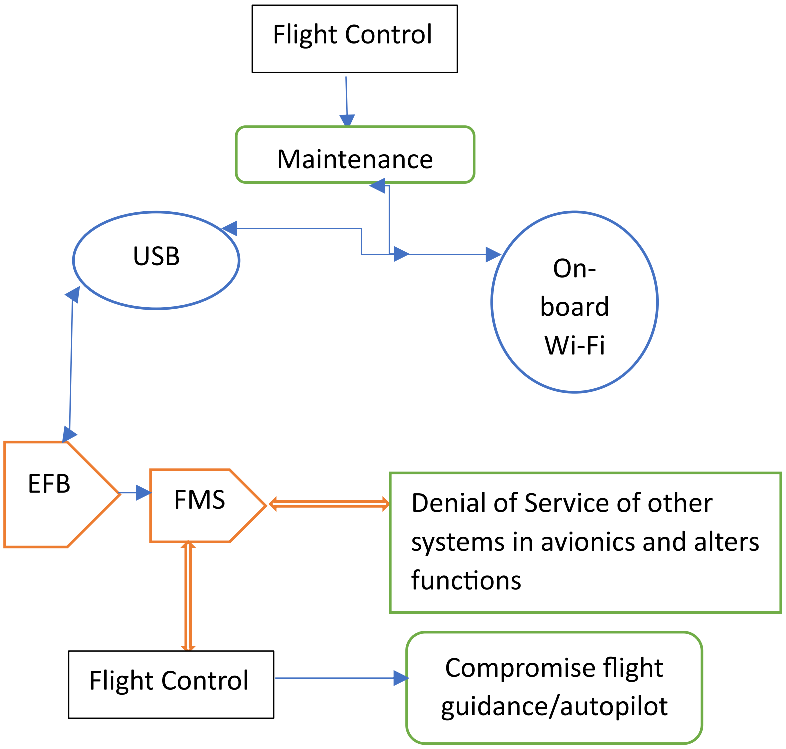
access to Electronic Flight Bag (EFB) from the FMS which is bidirectionally interfaced to the crew device through this same Wi-Fi.
For the purpose of this evaluation, it is assumed that the pilot must visually confirm any flight plan upon initial load as part of ground-based checklists. Furthermore, similar checks apply during flight, requiring pilot approval to in-air modifications to the flight plan. However, these operational policies are prone to human error and offer no computational certainty. The primary outcomes from attacking the FMS include displaying misleading FMS information to the pilot, making unauthorized changes to the FMS database.



2. *Flight Control*

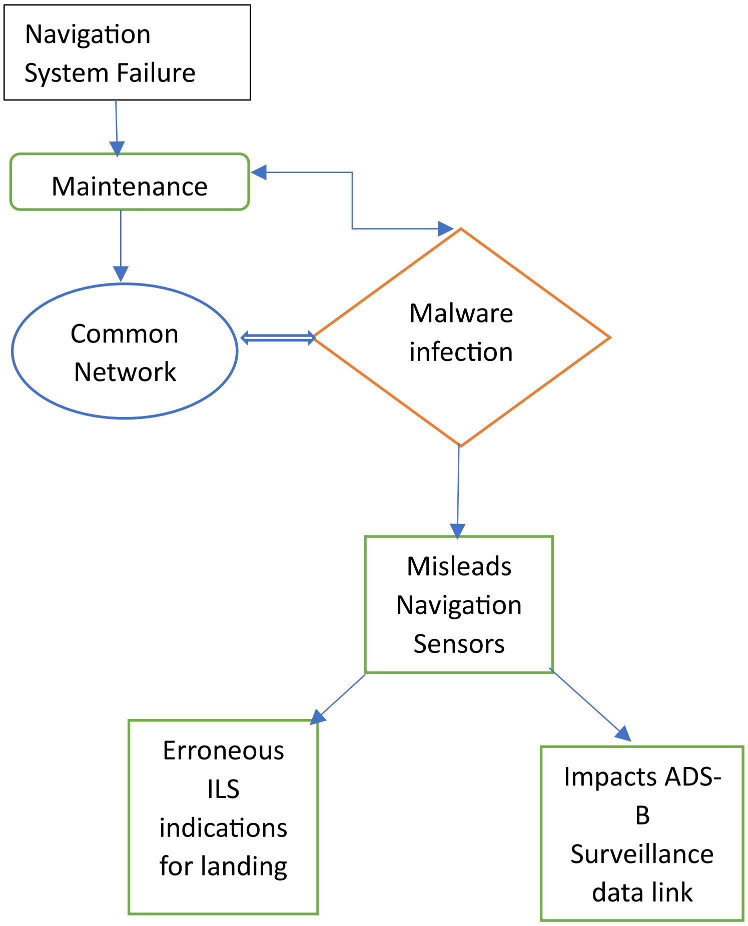
In this scenario, an attacker wishes to disrupt the Flight Control operations. This latest technology aircraft is equipped with avionic block that directly interfaces with maintenance through USB. Furthermore, enhanced capabilities of the ADFX standard (A664) are integrated to collect data about the condition of avionic systems to be provided to the maintenance crews so that issues can be resolved quickly.

For the purpose of this exercise and given the architectural flow, the maintenance personnel connect their tablet via USB or on-board Wi-Fi for routine monitoring of the avionic systems' hardware and software for faults and for overall health monitoring. This tablet/laptop is the primary maintenance system user interface that is used to update or change software configurations. A malware could be installed on an Electronic Flight Bag (EFB) which is integrated with FMS. Due to the bidirectional data flow through A664 using the shared network and integrated nature of this architecture, the malware could laterally propagate from FMS to other critical systems. Stealthy malware can manipulate maintenance records or inspection reports, thereby concealing issues with the systems that could pose a safety risk. This can lead to serious situations where the aircraft is deemed safe to fly, but in reality, it has critical issues that would be problematic during the flight. Additionally, if this malware is programmed to be time-bombed (logic-bombed), and once the aircraft is in the air, it could trigger to alter flight plans, position, tamper with the navigation database, set of communications, affect health management, hydraulic system, thereby compromising the flight guidance provided by the FMS to the Flight Control System which can be catastrophic.
It is important to note that I have excluded the hardware supply chain case for MRO.


Flight Control
Maintenance
USB
On-board Wi-Fi
EFB
FMS
Denial of Service of other systems in avionics and alters functions
Flight Control
Compromise flight guidance/autopilot

3. *Navigation System*

In this scenario, an attacker wishes to compromise the aircraft's navigation capability.
Based on the given architecture, the maintenance personnel injects dormant malware before flight takeoff via network means through the communications bus. This malware is activated when the aircraft is on active ILS (Instrument Landing System) approach to a runway and low to the ground. The malware causes the navigation sensors to capture erroneous ILS indications and coordinated navigation indications which makes the aircraft appear to be on course for the runway, but actually be flying into the ground away from the airport. Erroneous navigation data is also passed to the communications surveillance system (ADS-B OUT in this case) which decreases the likelihood that the air traffic controllers will notice the aircraft's true position.
This puts aircraft flight safety at risk, especially for landing at night or in bad foggy weather.


Navigation System Failure
Maintenance
Common Network
Malware infection
Misleads Navigation Sensors
Erroneous ILS indications for landing
Impacts ADS-B Surveillance data link

These attack trees characterize individual threats that represent attack scenarios as discrete exploitation steps in a tree structure. Each path through the tree elaborates the ways an attacker could cause an event to occur as shown above. Attack trees consist of

1. Tree root (goal of the attack),
2. AND/OR leaf node(s) (conditions where the attack will succeed if one or more conditions are satisfied),
3. Preconditions (skill level of an attacker, access to the system, resources available),
4. Postconditions (results of a successful attack such as gaining access, changes made to the system)

<u>Assessment of Risks:</u>

The airworthiness security risk assessment is organized according to threat scenarios, each of which classifies the pertinent information about potential successful attacks. I organized threat scenarios in terms of:

a. source of the attack in terms of security environment,
b. identification of an attacker and the security perimeter,
c. track of the attack path through the architecture up to the asset,
d. final threat conditions that are the effects of the successful attack.

For the purpose of risk assessment, I utilized several attacker characteristics to identify the minimum qualitative characteristic of an attacker necessary to complete an attack objective. The four attacker characteristics used are resources, access, cyber knowledge, and avionics knowledge.

Resources include factors such as available time, commitment for research, team size, and money. Access includes both physical access to the aircraft, but also virtual access via supporting infrastructure. The characteristic of knowledge represents the domain knowledge and experience necessary to understand and complete an attack objective. And so, for the purpose of this exercise, I break the knowledge characteristic into two distinct categories: cyber knowledge and avionics experience. These characteristics represent the two distinct domains of knowledge. For instance, the three attack scenarios described would utilize traditional security vulnerability analysis tools, and merely require security experience, but would require avionics specific knowledge to understand the system operation. That might include a special understanding of processes and procedures, system functions, real-time operating systems, buses, etc.

To calibrate these attacker characteristics, I used a taxonomy of hackers to generate a sample attacker rubric.

Attacker Type	Resources	Access	Cyber Knowledge	Avionics Knowledge
Script-Kiddies	Low	Low	Low	Low
Insider	Low	High	Low	High
Grey Hats	Low	Low	High	Low
Professional Criminals	High	Medium	High	Medium
Hacktivists	Medium	Low	Medium	Low
Nation State	High	High	High	High

**While nation state attackers may have ultra-access, it is considered beyond the scope of this exercise.*

Currently, no universal quantitative security metric exists, and so for the purpose of this exercise, I devised a simple technique for scoring attack trees by determining the path of easiest penetration and evaluate the overall risk.
I represent this score as 4-tuple defined as (resources, access, cyber knowledge, avionics knowledge). Each element of the tuple is assigned a distinct score, where 0= lowest requirement, 3=highest requirement. For instance, the tuple (1, 3, 2, 0) represents low resources, high access, medium cyber knowledge and no avionics knowledge. Accordingly, I calculated scores for these three attack scenarios:

Flight Management System (FMS)
Attacker Type= Professional Criminal (Passenger)
Threat Score= (3, 2, 3, 2)

Flight Control
Attacker Type= Insider (Maintenance Personnel)
Threat Score= (1, 3, 0, 3)

Navigation System
Attacker Type= Insider (Maintenance Personnel)
Threat Score= (0, 3, 1, 2)

**In practical real scenarios, there can be dependencies considering the resources, access, cyber and avionics knowledge characteristics. Also, considering the complexity of supply chain and stakeholders, a combination of attacker characteristics may come into play. For example, an insider can also be a nation state, hacktivist, or a script-kiddie. Hence, the overall threat landscape and risk may be subject to change.*

This exercise classifies the threat conditions severity that immediately contribute to the airworthiness of the aircraft, and further classifies the severity of the impact of all the events in terms of top-level conditions. This report considers the following classes of threat conditions:

Class of Threat Condition	Definition
Loss of Confidentiality	Exposure of Information
Unintended function	Unintended function is performed; this includes the presence of malware
Tampered information	Intended function appears to be performed correctly but is incorrect but satisfies safety integrity mechanisms. Includes coherent corruption.
Spoofed Information	Intended information appears to be correct and correctly sent, but either source or destination is incorrect.
Misuse	An intended function being invoked by an unauthorized entity.
Counterfeiting	Tampering with persistent data, including but not limited to coherent corruption of software part or user modifiable data.

Determination of Likelihood of Occurrence:-

The level of threat of a threat condition is determined by its likelihood which is measured by the qualitative evaluation of how often a successful attack might occur. This is based on probabilities as Frequent, Probable, Remote, Extremely Remote, and Extremely Improbable (not on the derived probabilities per flight hour) as defined by DO-356.

Determination of Severity Levels:-

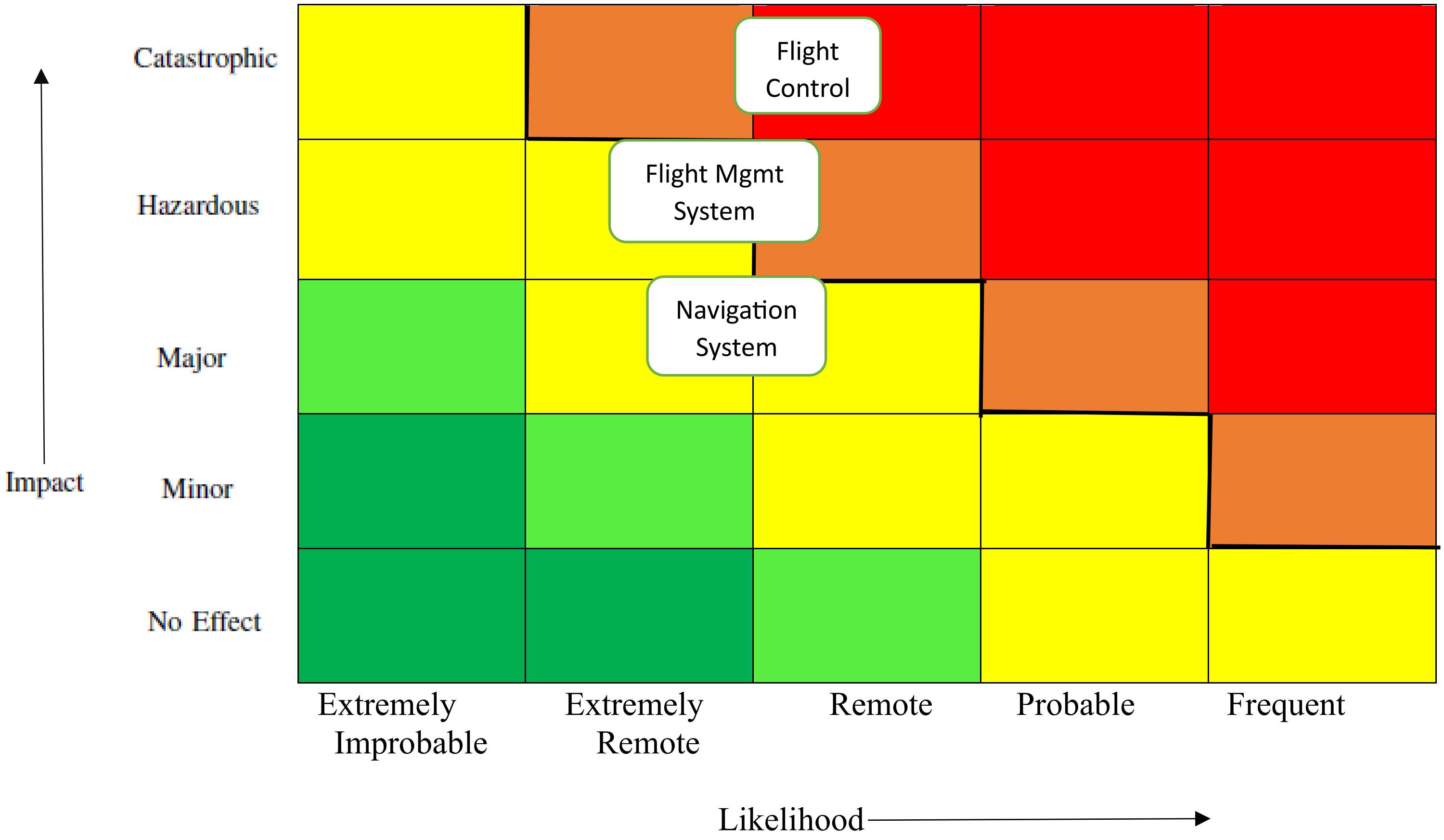
The determination of the impact magnitude is considered as the assessment of the severity of effects caused to assets (aircraft) by the successful attack. In this exercise, the threat severity levels are classified as Catastrophic, Hazardous, Major, Minor or No Safety Effect as defined by AC/AMJ 25.1309.
The resulting severities and scores are correlatingly representing the maximum impact on the safety of the aircraft as shown below.

Threat	Severity	Score
Flight Management System	Hazardous	(3, 2, 3, 2)
Flight Control	Catastrophic	(1, 3, 0, 3)
Navigation System	Major	(0, 3, 1, 2)

Determination of Risk Level:-

Within current aircraft regulations, the level of risk unacceptability is expressed by classifying the adverse effect according to the severity category and requiring that the occurrence likelihood for each severity category be less than a mandated likelihood. Therefore, if the minimum requirement is met, the risk level is considered *Acceptable* and if the threat scenario occurs with the frequency higher than minimum required for the given severity, the risk level is defined with using one of the four levels: Low, Medium, High, Extremely High and are considered *Unacceptable* for the given design.

In this case, based on the severities and the scores, a subjective risk matrix is developed. As shown below, the thick black line, starting between the catastrophic border between extremely improbable and extremely remote and stair stepping down and to the right to the frequent border between minor and no effect represents the risk acceptability based on DO-356.



Risk Matrix

As shown in the above figure, threat scenarios for Flight Management System and Flight Control are currently identified to be *unacceptable*, while the threat scenario for Navigation System is marginally *acceptable*.

Mitigations in terms of Security Architecture:

Based on the risk assessment results, I propose to implement the following security measures in the architecture to ensure an acceptable level of safety:-

1] Segregation

For this aircraft, three basic domains have been defined and no information exchange is allowed if it's not required.

Aircraft Control Domain	**Information Services Domain**	**Passenger information & entertainment services domain**
- Avionics	- EFB - Maintenance systems - Air-ground based comms	- IFE - Onboard Wi-Fi - Personal devices (laptops/tablets)

The passenger domain must be physically and logically isolated from critical flight avionics systems. Given that the passengers and the flight crew- are on the same Wi-Fi provided by the external airline network, it is highly recommended to establish trust boundaries and establish a security perimeter. This is achieved by implementing proper networking measures such as filtering traffic through firewall and configuring VLANs (to isolate traffic for each group on LAN) across the aircraft network gateway to achieve segregation.

2] Integrity Checks

Digital Signature- It is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
As a security measure, integrity checks must be applied to the Field Loadable Software (FLS) across Flight Management System and Navigation System as a measure to detect data corruption, which includes the damage caused by unauthorized users, viruses, or other malware. A digital signature should be added on a loadable software part to guarantee the identity of the creator to the recipient. This ensures that the function on the system can determine the software part came from a recognized, untampered, valid source and can provide immunity from various attack paths introduced anywhere in the supply chain or the connection of maintenance devices as well as the process of software

distribution and update through electronic means (wirelessly or via a maintenance laptop).
Furthermore, measures must be taken to make unauthorized use of wireless maintenance laptop difficult to accomplish and easy to detect through strong vetting and vendor management security process.

3] <u>One way communication</u>

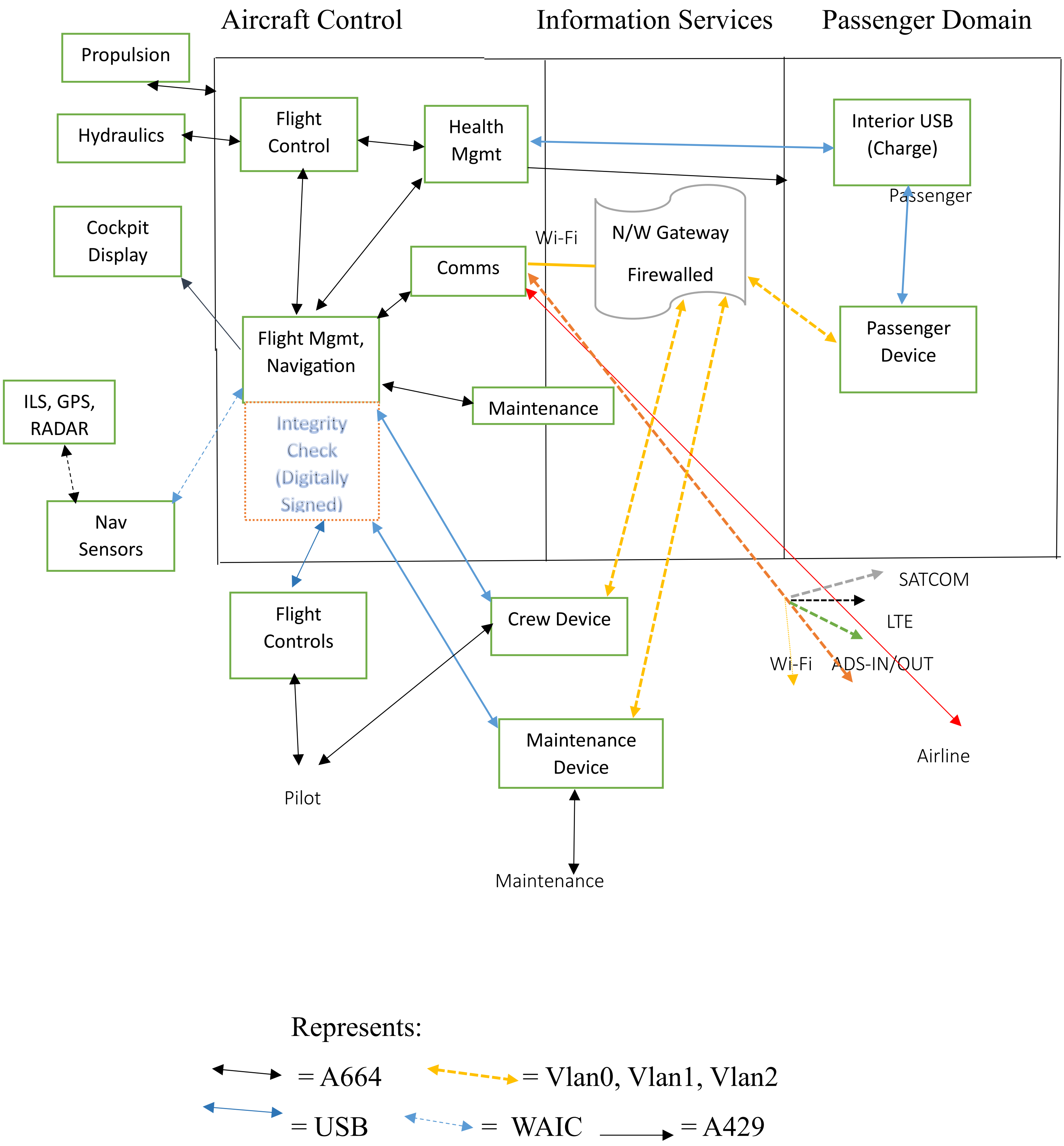
This is a measure that can guarantee the isolation of networks or limit network access. In the architecture, from the security perspective, it is advisable to establish a read-only (one-way) channel by incorporating cost-effective A-429 bus from the information services domain to the passenger domain so that passengers can receive flight updates. This would ensure that the systems would not be able to issue commands that directly control the aircraft.

4] <u>Authentication of communications and entities</u>

This model relies on several communication links and technologies to perform key functions such as sending and receiving data related to flight routes, landing, position, speed. Many of them are unencrypted and without authentication. For example, ADS-B. This means that these communication systems would be vulnerable to message injection, jamming, spoofing, replay attacks. I have not demonstrated such attack scenarios (with an airborne attacker) in this exercise. To tackle challenges with ADS-B, multilateration and frequency hop spread spectrum are a few of several countermeasures but are tedious to implement and costly. For other communication entities, public key infrastructure (PKI) will be an essential implementation.

**Optionally, it is advisable to implement and maintain aircraft security logs that specify the frequency, methods of storage, and retrieval. This is to be analyzed for anomalies to understand normal system behavior and identify security risks. It is also beneficial to create duplicate log files, one for immediate analysis and one for unaltered history.*

Proposed Changed Architecture:



Proposed Verifications:

Following the above proposed model and risk mitigation measures for the attack scenarios, it is essential to evaluate effectiveness of the means of remediation through the combination of the following:-

- ➔ Perform thorough penetration testing from the perspective of a potential adversary. For instance, running an adversarial simulation exercise as an airborne attacker performing attacks to compromise the network gateway, and gaining a foothold on crew device through MAC spoofing, ARP poisoning, man-in-the middle or other wireless attacks. This can be accomplished using traditional security vulnerability assessment toolkits.
- ➔ Conducting device/system level analysis on management and navigation systems to look for potential anomalies and test the effectiveness of digital signatures when external stakeholders are interfaced while running a compromised version of their software. In addition, it is also recommended to perform packet capture analysis within different avionics systems by intercepting the bus traffic flow from one system to another that would help to understand the nature of confidentiality of data within those entities.
- ➔ Routine audits, inspections, and reviewing the security measures and processes of maintenance vendors in the supply chain.

Conclusion: This report describes the methodology and results of performing an architectural security assessment on a commercial EASA CS-23 aircraft avionics system. When evaluated against the DO-356 risk level acceptability, attack vectors were introduced, and two threats were identified to be unacceptable; one marginally albeit acceptable. Based on their significant influence on the risk assessment, security measures were devised, and respective verification measures were proposed that do not affect the operational safety of the aircraft.

Reference(s):

Change information - AMC-20 Amendment 18 (europa.eu)

RA 5890 – Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design (publishing.service.gov.uk)

SafetyVersusSecurityStandards.pdf (dlr.de)

Certification Specifications (CSs) | EASA (europa.eu)

https://www.gao.gov/products/gao-21-86

https://huichawaii.org/wp-content/uploads/2019/06/Klim-Zdzislaw-2019-STEM-HUIC.pdf

Aviation Cybersecurity: Technology and Teamwork - YouTube