System Test Plan For:

Aircraft Network Domain Enhancement System

Allen Biagetti

Charles Gilmore

Maxwell Gorley

Anthony Johnson

Matthieu Privat

Jorge Santos

Jacob Stephens

Max Wilson

Version/Author	Date
1.0/MW	10/18/21
2.0/AJ and MW	12/1/21

Table of Contents

1. Introduction

1.1 Purpose

This document is a test plan for the Aircraft Domain Security Enhancement and its constituent components. It describes the testing strategy and approach to testing the team will use to verify that the application meets the established requirements of the FAA and security protocols before release.

1.2 Objectives

- Meets the requirements, specifications, and FAA regulations.
- Supports the intended business functions and achieves the required standards.
- Follows internal security and Boeing standards

2. Functional Scope

The Modules in the scope of testing for the Aircraft Network Domain Enhancement System are mentioned in the documents attached in the following path:

1. The System Requirements Specification document: W Group6_SRS.docx
2. The System Design Specifications document W Group6_SDD.docx
3. Section 3.1 of this document

3. Overall Strategy and Approach

3.1 Testing Strategy

Aircraft Network Domain Enhancement System will include testing of all functionalities that are identified by the scope (section 2). System testing activities will include the testing of new functionalities, modified functionalities, screen level validations, workflows, functionality access, testing of internal & external interfaces.

The testing types section following this one will discuss what needs to be tested. However, this section will describe how the types will be tested.

3.1.1 Application Testing

Test Objective: Software components and their inputs, processing, and outputs will function according to specified requirements in the SRS under section 4 for the components involved.

Technique: For software components, valid inputs should yield corresponding valid outputs leading to the validation of that test case.

Completion Criteria: When all test cases have been executed and only validated components exist in the final system.

3.1.2 Network Testing

Test Objective: Network components' connection, data transfer, and encryption will work according to the specified requirements in the SRS under section 4 for the components involved.

Technique: Network testing will be done using packet sniffing services such as wireshark to verify that communication is being completed as intended.

Completion Criteria: A connection can be validated upon a message being successfully sent from node to node. Data transfer can be validated if the message received matches the message sent. Encryption can be validated if desired encryption is applied to the message. When all test cases have been executed and only validated components exist in the final system.

3.1.2 Script Testing

Test Objective: Scripts and Subroutines for the system will execute according to the specified requirements in the SRS

Technique: Several script types will be used in this system. To validate them, they will run on the test network to make sure all parts execute without error.

Completion Criteria: Scripts will be validated upon executing every piece of software they are required to. Any programs that are not required shall not execute. When all test cases have been executed and only validated components exist in the final system.

3.2 System Testing Entrance Criteria

To start system testing, certain requirements must be met for testing readiness. The readiness can be classified into usability testing, functional testing, and data and documentation testing.

3.3 Testing Types

3.3.1 Usability Testing

User interface attributes and their content will be tested for accuracy and general usability. The goal of Usability testing in the context of this system is to ensure that User Interfaces for both the Aircraft Network and the Penetration Testing Kit are comfortable to use and provide the user with consistent and appropriate access and navigation through the system.

3.2.1: The Access Point shall host an SSH server

3.2.2: The Access Point shall take JSON files and ZIP files as inputs

3.2.3: The system shall output the status of uploaded files

3.2.4: TBD

3.3.2 Functional Testing

The objective of this test is to ensure that each element of the component meets the functional requirements of the system as outlined in the system features section. The subsections include functional requirements for the Gate Access Point, the Central Server, the TFTP Server, the Printer, and the Penetration Testing Kit.

3.3.1: The client shall connect to the Access Point via an SSH server

3.3.2: The Access Point shall send uploaded JSON files to the Central Server

3.3.3: The Access Point shall send uploaded ZIP files to the TFTP Server.

3.3.4: The Central Server shall maintain an ongoing network log

3.3.5: The Central Server shall host a web server

3.3.6: The Central Server shall send instructions to the Printer

3.3.7: The TFTP Server shall upload files to other computers in the network

3.3.8: The Printer shall print documents sent to it

3.3.9: TBD

3.3.3 Data and Documentation Testing

Data and documentation cover all the user guides, installation guides, read me files and set up a manual that is provided with the software to ensure that the user understands the Aircraft Network Domain Enhancement system. The objectives of this type of testing are to check if what is stated in the documents is available in the software, as well as check if the explanation of the system is correctly explained in the documentation.

3.5.1:

3.4 Suspension Criteria and Resumption Requirements

This section will specify the criteria that will be used to suspend all or a portion of the testing activities on the items associated with this test plan.

3.4.1 Suspension Criteria

If a network intrusion is detected, testing will cease immediately until the issue is resolved. Testing will also be halted if any incidents occur that will not allow for the system to perform testing.

3.4.2 Resumption Requirements

Resumption of testing will begin only after the network environment has been properly secured and reinitialized after a breach. In the case that an incident is halting tests from being conducted, the components involved will be fixed before testing resumes. Any changes in security should also be noted in case of further revision.

4. Execution Plan

4.1 Execution Plan

The execution plan will detail the test cases to be executed. The Execution plan will be put together to ensure that all the requirements are covered. The execution plan will be designed to accommodate some changes if necessary if testing is incomplete on any day. All the test cases of the projects under test in this release are arranged in a logical order depending upon their interdependency.

The test plan for the Usability Requirements:

Requirement (From SRS)	Test Case Identifier	Input	Expected Behavior	Pass / Fail
The Access Point shall host an SSH server	USE-T1.1	User connects with host ip and username. (Ex: ubuntu@ 123.123.123.122)	Upon established connection, a server status will output	PASS
The Access Point shall take JSON files and ZIP files	USE-T2.1	User uploads file via SFTP protocol	Server will respond that the file has been uploaded	PASS
The system shall output the status of uploaded files	USE-T3.1	User will upload file	Server will respond that the file has successfully been sent to its destination	PASS

The test plan for the Functionality Requirements:

Requirement (From SRS)	Test Case Identifier	Input	Expected Behavior	Pass / Fail
The client shall connect to the Access Point via an SSH server.	FUN-T1.1	User attempts to connect via SSH	User shall be prompted for a username or key passphrase	PASS

The Access Point shall send uploaded JSON files to the Central Server.	FUN-T2.1	Access Point attempts to upload JSON file to the Central Server	JSON file shall be downloaded in its original form	TBD
The Access Point shall send uploaded ZIP files to the TFTP Server.	FUN-T3.1	Access Point attempts to upload ZIP file to the TFTP server	ZIP file shall be downloaded in its original form	TBD
The Central Server shall maintain an ongoing network log	FUN-T4.1	User will request network log through network	Network Log as file will be downloaded	TBD
The Central Server shall host a web	FUN-T5.1	Once in network, user will search for web server in browser	Webpage for network will appear	TBD
The Central Server shall send instructions to the Printer	FUN-T6.1	User will request a file to be printed	Central Server will sent corresponding print request over network	TBD
The TFTP Server shall upload files to other computers in the network	FUN-T7.1	Gate Access Point will upload file to TFTP Server	TFTP Server will upload file to another computer in network	TBD
The Printer shall print documents sent to it	FUN-T8.1	Central Server sends print command and file to Printer	Printer will print file	TBD

Table 4.1. This table goes into detail about how to test each specific requirement from the System Requirements Specification document and includes what the expected result of the test should return.

5. Traceability Matrix & Defect Tracking

5.1 Traceability Matrix

List of requirements, with corresponding test cases:

Requirement (with severity)	*Test Case*

5.2 Defect Severity Definitions

Critical	The defect causes a catastrophic or severe error that results in major problems and the functionality is rendered unavailable to the user. A manual procedure cannot be either implemented or a high effort is required to remedy the defect. Examples of a critical defect are as follows: ● The system will not connect to the network ● The entire system cannot transmit data from one part to another ● Data is corrupted
Medium	The defect does not seriously impair system function and can be categorized as a medium Defect. A manual procedure requiring medium effort can be implemented to remedy the defect. Examples of a medium defect are as follows: ● Part of a system is malfunctioning but still online ● Code runs but does not do the intended task
Low	The defect is cosmetic or has little to no impact on system functionality. A manual procedure requiring low effort can be implemented to remedy the defect. Examples of a low defect are as follows: ● The system is not updated with the latest version ● The latest security enhancements are not pushed to the network

Table 4.2. This table lists the various levels of security and system flaws, along with examples.

6. Environment

6.1 Environment

▪ The System Testing Environment will be used for System Testing.

To conduct the testing, the tester needs to have the following installed onto their computer:

- QEMU Version 6.1.0
- Any up-to-date Linux Distro (Such as Ubuntu or Debian)
- ParrotSec Version 4.11.2
- VirtualBox Version 6.1.26
- TFTP for Linux Version 5.2+20150808-1ubuntu4_amd64.deb

7. Assumptions

This section list assumption that is made specific to this project:

- It is assumed that a high-speed broadband internet connection will be available so that all virtual machines can be managed.
- An additional assumption is that an SSH client will be installed on all computers trying to connect to the virtual machine network.

- The virtual machines depend on a sufficiently powerful Linux-based host with at least 16 gigabytes of RAM to run them.

8. Risks and Contingencies

Risk #	Risk	Impact	Contingency Plan
1	The ability of malware to escape the virtual network system	Critical	Isolate network and mitigate systems that have been affected by the malware. Inform IT if necessary or scrub the network for malware.
2	Malware compromises a major component of the AISD system	Critical	Report findings to Boeing and figure out a way to mitigate the issue.
3	Networking components fail during testing routine	Medium	QEMU will be halted and components will be individually tested before test resumes.
4	Emulated machine crashes during testing routine	Medium	QEMU will be halted. QEMU will be debugged until functional. Emulated machine will be tested before test resumes.
5	Software components dependencies aren't met	Low	Update software components to the latest version and continue tests.
6	The latest Linux OS update did not get updated before a test	Low	Update the OS to the latest version and re-run tests.

Table 4.3: Summary of risks and contingencies, along with their impact level.

9. Glossary

Term	**Definition**
AISD (Aircraft Information Services Domain)	A network intended for use by the aviation industry
Central Server	The primary server used to communicate with devices on the AISD network.
Gate Access Point	The machine that acts as the entry point into the AISD network.
JSON (JavaScript Object Notation)	Standard text based format for representing structured

	data based on JavaScript object syntax. Commonly used for transmitting data in web applications.
ParrotSec	A Linux distribution focused on penetration testing
QEMU	The virtualization environment used to emulate the machines on the AISD network.
RAM (Random Access Memory)	Type of memory your computer calls on for applications and data you’re currently using.
SSH (Secure Shell)	Works by the exchange and verification of information, using public and private keys, to identify hosts and users. It then provides encryption of subsequent communication.
TFTP (Trivial File Transfer Protocol)	Uses client and server software to make connections between two devices.