Aircraft Access to System-Wide Information Management Infrastructure

Mohammad Moallemi, Remzi Seker, Mohamed Mahmoud, Jayson Clifford, John Pesce, Carlos Castro, Massood Towhidnejad
Next Generation Applied Research Lab. (NEAR)
Embry-Riddle Aeronautical University
600 S. Clyde Morris, Daytona Beach, FL. USA
[moallemm;sekerr;mahmoudm;cliffj;pescej;castroc;towhid]
@erau.edu

Jonathan Standley, Robert Klein
Federal Aviation Association (FAA)
{jonathan.standley; robert.klein;paul.jackson}@faa.gov

Keywords: NextGen; AAtS; SWIM; Cybersecurity;

Abstract
Within the Federal Aviation Administration's (FAA) NextGen project, System Wide Information Management (SWIM) program is the essential core in facilitating the collaborative access to the aviation information by various stakeholders. The Aircraft Access to SWIM (AAtS) initiative is an effort to connect the SWIM network to the aircraft to exchange the situational information between the aircraft and the National Airspace System (NAS). This paper summarizes the high-level design and implementation of the AAtS infrastructure; namely the communication medium design, data management system, pilot peripheral, as well as the security of the data being exchanged and the performance of the entire system. The research work led to the design and implementation of a reliable data storing and exchange system between the Electronic Flight Bag (EFB) (pilot peripheral to the AAtS network) and the SWIM network architecture. Issues such as cyber-security, performance, availability, and quality of service in the AAtS are investigated and mitigation approaches toward more secure and efficient service provided to the aircraft and to NAS are discussed.

1. INTRODUCTION

The Federal Aviation Administration's (FAA) Next Generation Air Transportation System (NextGen) program [1] is a long-term modernization and transformation of the current National Airspace System (NAS) into a more effective, coordinated, and collaborative decision-making system. It will provide a more reliable, secure, and dependable aviation capability for both users and operators, which ensures more capacity, throughput, while maintaining the high level of safety.

System Wide Information Management (SWIM) [2] is one of the NextGen components designed to use a Service Oriented Architecture (SOA) technology that communicates aviation data among the various stakeholders and allows the implementation of several concepts such as trajectory based operations and optimum profile descent, among others. SWIM allows several different NextGen technologies to exchange data without worrying about specific requirements and restriction of the target environment.

A current developing NextGen technology is the Aircraft Access to SWIM (AAtS) technology which provides methods and tools for real-time access of an aircraft flying in the national airspace (and in future globally) to the SWIM-enabled systems. AAtS is an air-to-ground communication infrastructure standard that provides the aircraft crew with the updated National Airspace (NAS) information and vice-versa. Currently, the lack of such an infrastructure poses the following risks to the national aviation operations [4]:

1. Heavy reliance on voice communication which poses risks such as read back clarity and frequency interference.
2. Lack of real-time weather modeling, aeronautical, and traffic information to the crew during the entire flight phase.
3. Lack of real-time access to flight information and weather information provided by aircraft sensors or crew by the Air Traffic Management (ATM).
4. Risks caused by inefficient collaboration in decision making process by the stakeholders due to the lack of comprehensive real-time National Airspace (NAS) data.

Figure 1 illustrates different components of the AAtS infrastructure within the NextGen program. These components are described in the next subsections. One of the potential benefits from AAtS is less reliance on legacy voice communication for decision making by

the crew and more situational awareness by providing operational data through digital means. AAtS defines the standard for interfacing SWIM shared services to the aircraft during all phases of the flight by defining the technical and operational requirements. This architecture will provide the aircraft crew with the most updated and real-time aeronautical data provided by different aviation stakeholders such as FAA, Department of Homeland Security (DHS), airports and other information sources publishing into SWIM.

In this paper we discuss the high-level issues in design and development of the AAtS system, its components, as well as the cybersecurity issues concerning the data transfer in AAtS. Delivering the National Airspace (NAS) data to the Electronic Flight Bag (EFB) (the onboard client AAtS interface to the crew) and vice-versa is the major focus of the AAtS project which will be elaborated here. In this project, we designed and programmed the main components of AAtS as well as an emulated network that replicates the functionality of the AAtS and necessary System Wide Information Management (SWIM) components for testing purposes. AAtS specifications can be found in [1], [3], and [4].

AAts is composed of three major components: Aircraft Interface Peripheral, Data management Service (DMS), and The Data Link Service (DLS).

In the context of NextGen, Aircraft will be majorly a consumer of National Airspace (NAS) data, through the EFB available to the pilot and the crew. It is also planned to be a NAS service provider by supplying sensor data as well as visually conceived weather information provided by the crew (e.g. pilot report (PIREP)).

DMS is the data provider for the Aircraft via the DLS and is responsible for managing the data flow between the NAS Enterprise Security Gateway (NESG) to the aircraft. DMS manages the access and services among the shared data providers and the data consumer (aircraft).

DLS is responsible for the network connection between the DMS and the aircraft, which includes, providing the network services as well as routing the data via the appropriate protocol and path. Currently the main internet connection to the aircraft is provided by means of ground to air cellular network towers as well as satellite connection [6].

Information is exchanged within the context of the AAtS between the DMS and the aircraft. These information exchange scenarios are classified in nine categories by FAA in [5]. These data exchange scenarios are also called “operational scenarios” (OS) and are listed here.

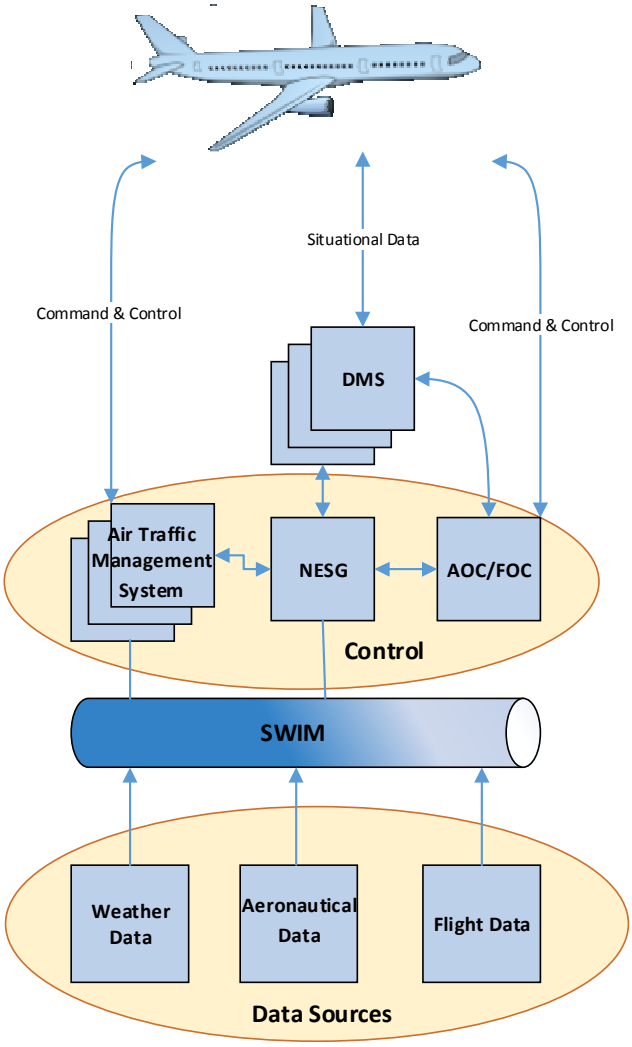

Figure 1. NextGen Air-Ground Communication

- **OS1: Trajectory Information Exchange**
- **OS2: Weather Modeling**
- **OS3: Automated Flight Service Station (AFSS)**
- **OS4: Special Activity Airspace (SAA)**
- **OS5: Automated Flight Conditions Report**
- **OS6: Airport Diversion Planning**
- **OS7: Surface Management with Trajectory Based Operations**
- **OS8: En-route Strategic Planning**
- **OS9: Learning-Capable Decision Support Tool**

Several of these scenarios are already operational within the framework of SWIM and the data is available on the DMS to serve the subscribed clients, such as AIRMETs (Airmen's Meteorological Information), SIGMETs (Significant Meteorological Information), PIREPs (Pilot Report), METARs (Meteorological Information), and NEXRAD (Next-Generation Radar). However, not all of the OS' are functional, e.g. SAA. Therefore, the scenarios make some relevant assumptions regarding the size and frequency of the data to perform desired tests.

Three Technical Scenarios have been defined in [5]. These TS are as follows:

- TS1: Publish/Subscribe Service – defines that the information is sent at a predetermined update rate on a continuous fashion.
- TS2: Event Triggered – defines that the information is sent as it is created.
- TS3: Request/Reply – defines that the information is sent when it is requested

Four Messaging Patterns are identified as potential for NAS services and the DMS to achieve connectivity with the EFBs [5]. These messaging patterns are

- MP-A: NAS Service Hosting a Web Service Operation -the NAS service provides a web service function to openly receive aircraft data from the DMS.
- MP-B: DMS Hosting Request-Response Web Service
- MP-C: DMS Hosting Pub-Sub Service using JMS
- MP-D: DMS Hosting Pub-Sub with Web Service Notification

MP-A is out of scope of our research as our research focuses on connectivity between the EFB and DMS.

2. AATS DESIGN AND IMPLEMENTATION

In general, AAtS provides the following two services:

- NAS services to the crew via SWIM infrastructure
- Ground-to-air information exchange between aircraft and NAS services

Different entities are involved in the data exchange between the Aircraft and the SWIM-enabled services. The rest of this section discusses these components.

2.1. Aircraft Interface Peripheral (EFB)

The EFB is an iOS based application that communicates with the DMS and is responsible for providing real-time weather data directly from FAA subscribed resources. This communication is handled by a network protocol called (Data Management Service Protocol Interface) DMSIP developed in our lab. DMSIP is an application level messaging protocol for interfacing with the DMS in order to access available data and services. The protocol is designed to be adaptable through extensions of its request methods, status codes and message fields. Any transport layer protocol may be used with DMSIP as long as it provides bi-directional communication. In addition, each message is encoded as JavaScript Object Notation (JSON) and transmitted. Figure 2 illustrates the connectivity path between the DMS and the Electronic Flight Bag (onboard an aircraft) that is provided by a Data Link Service Provider (DLSP).

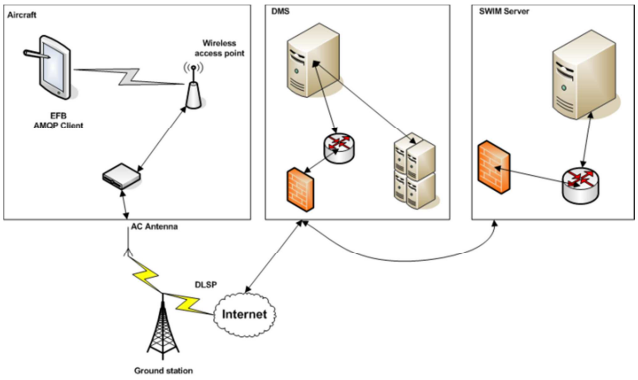

Figure 2. EFB Physical Connectivity Layout

2.1.1. User Interface Design

The EFB main interface is composed of three main user interface components; the authentication, the map and information view, and the product selection view. The authentication allows the user to login to the system as a valid crewmember, connect to the DMS Server, and display the connection status. The map and information view displays the base map and the different products based on the user product selection. The map is zoomable and dynamically updated with relevant subscribed information. The product selection view allows the user to select between different products and subscribe to automatic updates of the desired information as well as to change the map type. Figure 3 shows a snapshot of the general layout of the EFB application.

2.1.1. System Design

The EFB application is composed of two primary components: a User Interface module (UI) that allows the user to input and display requested data, and the

World module, which establishes communication with the DMS, handles data requests, and updates data. The Model View Controller pattern (MVC) is the primary design pattern, where the controller manages the data flow between the World module and the UI and provides a predefined interface for the View to request data from the world module.

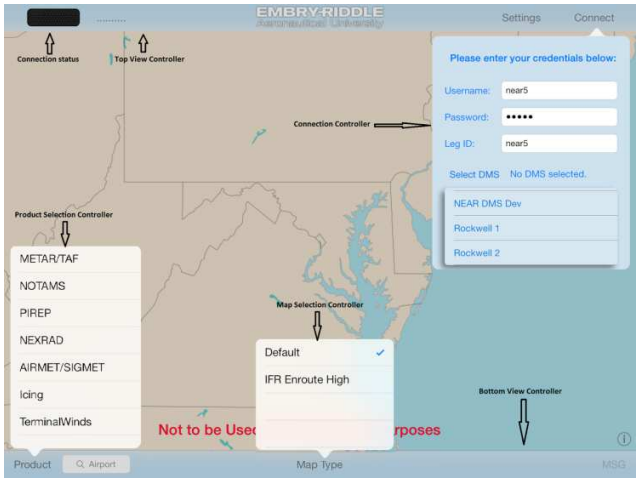

Figure 3. EFB UI General Layout

2.2. Data Management Service (DMS)

The DMS is responsible for accessing SWIM data and managing the flow of data to the aircraft, via the data link service (DLS), as well as the synchronization of the data flow with the commercial carrier's operations control center. The system is designed to serve two types of clients:

- Aircraft
- Airline dispatchers

The DMS includes:

- Development servers
- Production servers
- Support equipment

The DMS development effort has produced three major versions of the system. The third version, DMSv3, incorporates lessons learned from a series of demonstrations with a commercial airline partner.

2.2.1. DMS Architecture

The DMS contains a message processor and caching server for storing data and servicing requests as efficiently as possible. Connections to the DMS are made SSL socket to increase the security of the entire data transfer to AAtS. This provides both publish-subscribe and request-response messaging patterns on a unified interface. The set of operations available on this interface are known as the DMS interface protocol (DMSIP) providing the data transfer between the DMS and the EFB. Any number of airline operations control centers or EFB clients can connect to the DMS with DMSIP underlying protocol. In addition, AAtS Data including weather data and aeronautical information is stored in the DMS using the same protocol. Figure 4 depicts an example weather data transfer scenario between the weather data provider and the EFB or the airline operations control center.

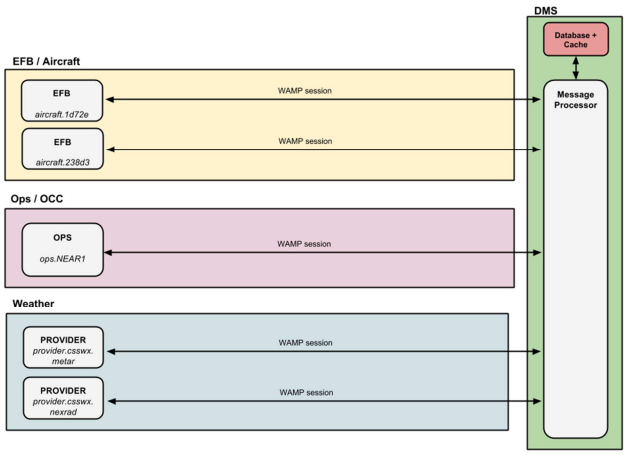

Figure 4. Example DMS Data Transfer

2.2.1. Data Retrieval and Subscription

Once the user selects a particular product, the EFB translates the requested data item into a Uniform Resource Identifier (URI). Each data resource stored in the DMS correlates to a unique URI. The EFB preloads the product associated with the URI using DMSIP. Along with the product information request, the EFB is also subscribed to each product ensuring the receipt of available product update notifications provided by the DMS.

The EFB uses two methods to find outdated resources:

- Receiving a DMSIP event from the DMS notifying it of changes to the subscribed resource, the EFB evaluates the resource version and if necessary, updates the product via remote procedure call (RPC).
- A periodic routine updates the EFB State Object and executes a bulk request for the versions of the resources to which the EFB is subscribed. If any resource is found to be out-of-date, the EFB acts to update the resource using the standard update procedure.

Any updates the DMS determines are necessary to send to the EFB generate notification messages that

are sent to the EFB. If the EFB wishes to update, it retrieves the resource via RPC. In this way, only notifications of changes are transfered over the pub/sub pattern, with all transfer of resource data occurring solely over RPC at the direct command of the EFB.

2.3. Data Link Service (DLS)

In general, the content rich AAtS services require a higher bandwidth Internet Protocol (IP) based Data Link. The most common IP Data Link types in use are Code Division Multiple Access / Evolution Data Optimized (CDMA/EVDO) working in the context of 3G and 4G cellular networks, or satcomm based products targeting business jets and commercial carriers. The CDMA/EVDO services are currently limited to use greater than 10,000 feet Above Ground Level (AGL) over the Continental United States (CONUS) and Alaska. Satcomm services offer mostly global coverage, but are limited to polar regions and over the ocean. Typical installations include a Wi-Fi router / access point and an air-to-ground modem with one or more SSIDs for use in the cabin and cockpit. Business jet solutions are typically marketed to the business jet operator, which may in turn provide service to their customers. Commercial carrier solutions typically market directly to the carrier's customers and may include service for the carrier.

Current popular satcomm based services can range in bandwidth between 32 and 650 Kbits/s, whereas cellular-based services can reach as high as 9.8Mbits/s per aircraft. Emerging hybrid technologies promise peek speeds of 60 Mbits/s or more over North America.

In the AAtS concept, communication between the EFB and the DMS is managed for an aircraft's available Data Link bandwidth. In general, the Data Link can be treated as a segment of the Internet between the EFB and the DMS.

3. SYBERSECURITY OF AATS

The focus of the cybersecurity aspect of AAtS is to identify the potential vulnerabilities and technical constraints associated with the use of Electronic Flight Bags (EFBs) and related cockpit data services on the flight deck. In addition, the information designated for the flight deck needs to be protected against threats, therefore we identified the potential security threats.

Figure 5 shows a detailed network structure of a typical AAtS technology. In this architecture, the cabin network and cockpit connectivity are shown, where a wireless connection is provided in the cabin area, vs. a wired or wireless connection for cockpit. A Data Link Service Provider (DLSP) proxy separates and routes the cabin vs. cockpit traffic to the internet. Thereafter, the cockpit traffic is routed to the DMS proxy where it can access the DMS server through a firewall.

A list of threats with potential mitigation scenarios to address are identified within the context of AAtS architecture. The followings are the identified threat details:

1. TH1: Improper traffic originating from the EFB utilizing majority of the bandwidth available in the DLS resulting in Denial of Service (DoS).
2. TH2: Cabin user gaining unauthorized access to DLS and conducting DoS through extreme consumption of the bandwidth.
3. TH3: Cabin user gaining unauthorized access to Wireless Access Point/Router to change configuration settings.
4. TH4: Authenticated cabin user consuming the DLS bandwidth and conducting DoS.
5. TH5: Authenticated user conducting reconnaissance on the DLSPs network for mapping the network along with fingerprinting servers.
6. TH6: External DoS/DDoS attacks on the DLSP servers by using a discovered IP address/hostnames of servers on the DLSP's network.
7. TH7: Conducting DoS against the Wireless Access Point/Router onboard the aircraft. This is possible due to the specification of the IEEE 802.11 standard.
8. TH8: Man In The Middle (MITM) attacks on the EFB-DMS path. Rogue access point impersonating the onboard Wireless Access Point/Router to conduct MITM attack.
9. TH9: DoS/DDoS attacks against the DMS. Using DMS's IP address, DoS and DDoS can be conducted.
10. TH10: User in the cabin sniffing flight deck traffic, malicious user can sniff data packets that flow between the EFB and the Wireless Access Point/Router to inspect contents of the packets.
11. TH11: Attack on the certificate authority and rouge certificates.
12.

3.1. AAtS Performance Measures

Several of the Operational Scenarios (OS') are already operational within the framework of SWIM and the

data is available on the Data Management Service (DMS) to serve the subscribed clients. However, many of these scenarios are not yet operational.

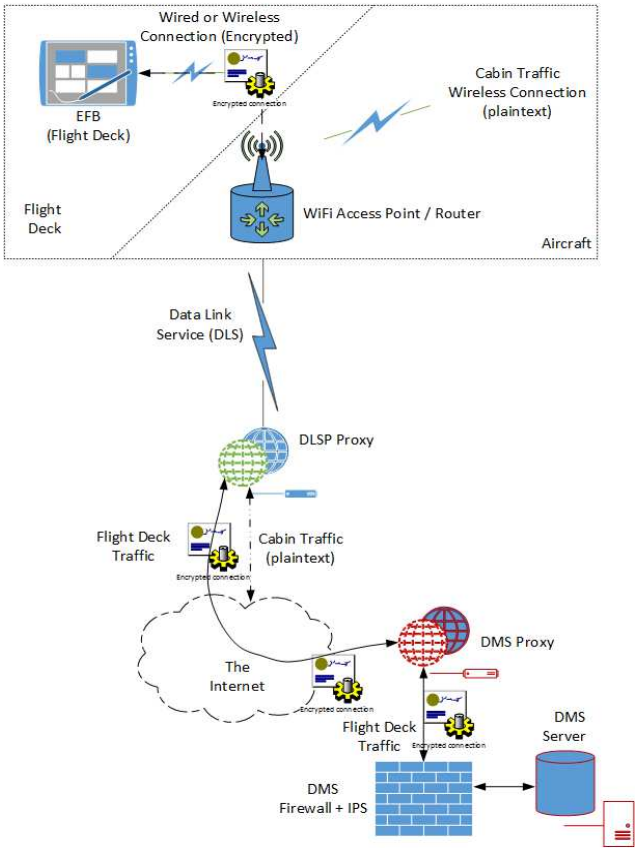

Figure 5. AAtS Network Architecture

A DMS server emulated the Technical Scenario (TS) and Message Pattern (MP) combinations. Data transfer within the selected OS' is emulated using files of appropriate sizes based on discussions with subject matter experts regarding sizes and frequencies of transfer. A series of data transfer operations were conducted, including initiating large numbers of operations in order to stress the network/server while performance metrics were being collected. In addition, the rate of read/write operations with parameters such as transfer time and speed were also recorded.

For testing purposes, only the efficiency of raw data, as it is transmitted between the aircraft and the SWIM database, was considered. This provides a controlled environment where the exchanged data was observed through a bandwidth-capped network. The DMS and EFB are the end to end nodes for these tests.

For each MP, timers are used to measure the time it took to transmit a fixed amount of data through the network. The network is given a specified bandwidth cap to simulate real world constraints in uplink and downlink scenarios. Using the total size of data transmitted, and the time taken to receive the data, the Client can calculate the effective transfer rate of the message exchange pattern.

4. CONCLUSIONS

The research project presented the development of a new concept in digital aviation, in which electronic flight bag has been programmed to interface the data updates between the aircraft and the ground stations. The paper presented details of the components and sub-systems of this technology as well as the research carried out to determine the cybersecurity of the entire system. The AAtS initiative by FAA has proved its application in revolutionizing the information transfer between the aircraft and the ground stations, thus improving the decision-making process of both parties. The cyber security investigation also detailed all the imminent threats to this system, tested the replicated network architecture and provided mitigation approaches to minimize the effect of such threats.

5. ACKNOWLEDGEMENT

This study was conducted in support of, and with the assistance of the US Federal Aviation Administration's Aircraft Access to SWIM program. This effort is part of the FAA's NextGen initiative.

6. REFERENCES

[1] "NextGen Implementation plan" FAA report June 2013.

[2] Jere S. Meserole, and John W. Moore. "What is System Wide Information Management (SWIM)?." Aerospace and Electronic Systems Magazine, IEEE 22.5, pp 13-19, 2007.

[3] "Aircraft Access to SWIM (AAtS) Concept of Operations (ConOps)", FAA technical report, July 31 2013.

[4] "Aircraft Access to SWIM Implementation Guidance Document", FAA technical report, March 1 2013.

[5] "Aircraft Access to SWIM Full Data Exchange Technical Concept Paper", FAA technical report, July 31 2013.

[6] W. S. Mossberg, "Internet-a-Gogo: Airlines to offer in-flight access." The Wall Street Journal, 2008.