DOT/FAA/TC-14/29

Office of Aviation Research
and Development
Washington, DC 20591

Investigate Security Vulnerabilities for a Representative Aircraft

Date: 08/14/2014

Type of Report: Technical Report

This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161.

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-14/29		

4. Title and Subtitle	5. Report Date
Investigate Security Vulnerabilities for a Representative Aircraft	August 14, 2014
	6. Performing Organization Code NA
7. Author(s) Terry Davis, Dennis Glatting, Eric Jacobs, and Luigi Valentini	8. Performing Organization Report No. Deliverable 0002
9. Performing Organization Name and Address Micro Systems Automation Group (MSAG) 2785 Hartland Road Falls Church, VA 22043	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTFAWA-11A-00037/0002
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Office of Aviation Research and Development Washington, DC 20591	13. Type of Report and Period Covered April 2014 - September 2014
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report provides the findings of the ongoing review of cyber security work in industry and other parts of government. It identifies potential areas where aircraft may be vulnerable to cyber-attacks, and recommends methods to test for actual vulnerabilities. This reports also details aircraft components and interfaces with an analysis prioritizing potential security issues and their level of effect on aircraft.

Short summary of report

The purpose of this study is to provide the FAA Tech Center with an initial analysis of cyber threats to the current generation of e-Enabled or connected aircraft, and to provide prioritized recommendations for follow-on research and industry guidance. Additionally, the study identifies common threats to legacy, current, and the next generation of aircraft.

17. Key Words	18. Distribution Statement
Aircraft security; cyber risks, cyber attacks	This document should be distributed and reproduced under the FAA approval and authority.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	84	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	vii
1. INTRODUCTION	1
1.1 PURPOSE	1
1.2 BACKGROUND	1
1.2.1 Aircraft Architecture	1
2. AIRCRAFT CLASSIFICATIONS	5
2.1 LEGACY AIRCRAFT GENERATION	5
2.2 CURRENT GENERATION (CONNECTED A/C)	5
2.3 NEW GENERATION	5
3. AIRCRAFT ARCHITECTURE	7
3.1 AIRCRAFT CONTROL DOMAIN (ACD)	7
3.2 CURRENT ONBOARD COMMUNICATIONS BUSES	8
3.3 AIRCRAFT INFORMATION SERVICE (AIS)	10
3.4 PASSENGER INFORMATION AND ENTERTAINMENT SYSTEMS (PIES)	10
3.5 RISK ANALYSIS	11
3.5.1 Design, Manufacture, and Maintenance	11
3.5.2 Loadable Software	11
3.5.3 Airline Modifiable Parts	15
3.5.4 Internet Access Points	15
3.5.5 Aircraft Electronic Portable Maintenance Aids	16
3.5.6 Multi-domain Use of Air-to-Ground Links	16
3.5.7 Remote Maintenance Access	16
3.5.8 Aircraft Network Domains	16
3.5.9 Onboard Aircraft Control and Communications Wireless Systems	19
4. RECOMMENDATIONS	20
5. CONCLUSIONS	22

LIST OF FIGURES

Figure	Page
FIGURE 1. AIRCRAFT DOMAINS	2
FIGURE 2. AIRCRAFT ARCHITECTURE AND AREAS OF CYBER CONCERN	2
FIGURE 3. SOFTWARE END-TO-END DISTRIBUTION PROCESS	12
FIGURE 4. FIELD LOADABLE SOFTWARE BY AIRCRAFT	13

LIST OF TABLES

TABLE 1. AIRCRAFT TYPES WITHIN LEGACY AND NextGEN ARCHITECTURES 5
TABLE 2. BUS TYPES USED IN AIRCRAFT 7
TABLE 3. FIELD LOADABLE SOFTWARE IN BOEING AIRCRAFT 13

LIST OF ACRONYMS

AAtS	Aircraft Access to System-wide Information Management (SWIM)
AAtW	Airborne All the Way
ACARS	Aircraft Communications Addressing and Reporting System
ACD	Aircraft Control Domain
ACCESS	Advanced Cabin Entertainment and Service System
ACMF	Airplane Condition Monitoring Function
ACMS	Aircraft Condition Monitoring System
ADC	Air Data Computer
ADIRU	Air Data Inertial Reference Unit
ADM	Air Data Module
ADN	Aircraft Data Networks
ADSB	Automatic Dependent Surveillance – Broadcast
AEEC	Airlines Electronic Engineering Committee
AFDX	Avionics Full Duplex Ethernet
AHM	Aircraft Health Monitoring
AIS	Aircraft Information Systems
AISD	Aircraft Information Systems Domain
AMI	Airline Modifiable Information
AOA	Aircraft Communications Addressing and Reporting System (ACARS) over Aviation VHF Link Control (AVLC)
AOC	Airline Operational Control
APTs	Advanced Persistent Threats
ARINC	Aeronautical Radio Incorporated
ASCPC	Air Supply and Cabin Pressure Controllers
ATC	Air Traffic Control
ATN	Aeronautical Telecommunications Network
AVLC	Aviation VHF Link Control
AVM	Airborne Vibration Monitor
CMU	Communication Management Unit
COTS	Commercial-off-the-shelf

CPDLC	Controller-Pilot Data Link Communications
CRADA	Cooperative Research and Development Agreement
CRCs	Cyclic Redundancy Checks
DME	Distance Measuring Equipment
DNS	Domain Name System
DoS	Denial of Service
EFB	Electronic Flight Bags
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FD/AP	Flight Director/Auto Pilot
FMS	Flight Management System
GBST	Ground Based Software Tool
GPS	Global Positioning System
HF	High Frequency
HIRL	High-Intensity Runway Edge Lighting
IEEE	Institute of Electrical and Electronics Engineers
IFE	In-Flight Entertainment
IMA	Integrated Modular Avionics
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRS	Inertial Reference System
LAX	Los Angeles International Airport
LRU's	Line Replaceable Units
MC	Mission Computer
NAS	National Air Space
NDA	Non-disclosure Agreement
NextGEN	Next Generation
NO COMM	No Communication
OEM	Original Equipment Manufacture
OS	Operating System
PFDs	Primary Flight Displays
PIES	Passenger Information and Entertainment Services Domain

PKI	Public Key Infrastructure
PODS	Passenger Owned Devices
PODDS	Passenger Owned Devices Domain
RFID	Radio Frequency Identification
RIOC	Remote I/O Concentrator
RVR	Runway Visual Range
SATCOM	Satellite Communications
SC	Special Condition
SDR	Software Defined Radio
SFD	Standby Flight Display
SITA	Société Internationale de Télécommunications Aéronautiques
SNMP	Simple Network Management Protocol
SWIM	System Wide Information System
TACAN	Tactical Air Navigation
TCAD	Traffic and Collision Alert Device
TCP	Transmission Control Protocol
TDMA	Time-division Multiple Access
TFTP	Trivial File Transfer Protocol
TWU	Terminal Wireless Unit
TWLU	Terminal Wireless Local Area Network Unit
UAS	Unmanned Aircraft System
UMS	User Modifiable Software
US	United States
USB	Universal Serial Bus
VDL2 VHF	Data Link Mode 2 VHF
VHF	Very High Frequency
VL	Virtual Link
VOR/ILS	Very High Frequency Omnidirectional Range/Instrument Landing System
WAP	Wireless Access Points
WOW	Weight-on-wheels

EXECUTIVE SUMMARY

The design and implementation of onboard aircraft networks is highly proprietary and both the airframers and their suppliers limit sharing information. This information is only available to the Federal Aviation Administration (FAA) under very tight non-disclosure agreements (NDA) prohibiting its publication or disclosure in any form. Thus, this study focuses on the current generation of e-Enabled aircraft using publicly available information on the Boeing 787 (B-787) and Airbus 380 (A-380) as base models for the current generation of e-Enabled or connected aircraft. Both aircraft adhere to Aeronautical Radio, Incorporated (ARINC) standards for aircraft networks and connectivity. The foundations for the study include base SAE/ARINC standards for air data networks.

This study presents the general cyber threats that exist in legacy aircraft and the current generation of connected aircraft models with multiple network domains onboard, terminal wireless connectivity, Internet connectivity for passengers and crew, line-replaceable-units (LRUs) that are shared between aircraft domains, loadable software, electronic flight bags (EFBs), etc. Additionally, it covers threats that will be encountered with new technologies in the next generation of aircraft. It also covers the cyber threats that exist during the aircraft design process and through the supply chain during its manufacture.

Study results show that the aircraft is most vulnerable to five types of threats:

1. Manipulation of aircraft loadable software parts, and airline modifiable information (AMI) components.
2. Inadvertent or deliberate interconnection of aircraft domains during manufacture, maintenance, or modifications.
3. Unexpected vulnerabilities to attacks directed at aircraft, offboard communications links, or onboard aircraft wireless control and communication systems, including common attacks to penetrate aircraft domains and denial of communications services.
4. Manipulation of the aircraft's digital design and software components, during its design.
5. Insertion of backdoors or malware into aircraft electronic components or systems, via the supply chain during manufacturing.

The manipulation of aircraft loadable software parts and AMIs should receive the highest priority for further study and research. These threats apply to virtually all commercial aviation aircraft, and are used in legacy and current generation aircraft. In time, even more software parts and loadable virtualized systems will exist in the next generation of new aircraft. Follow-on work should create credible demonstrations of threats to these components; therefore, we recommend countermeasures to protect loadable software and AMIs. We further recommend initiating research into the specific vulnerabilities that virtualized systems and LRU will present in order to be prepared to author cyber guidelines. The vulnerability of existing aircraft communication links to unexpected cyber-attacks and conditions during link design should also be a high priority research task.

NOTE: A recent article posted on the Fox Business web site reports the work of a researcher conducting reverse engineering. This researcher discovered vulnerabilities by reverse engineering - or decoding - highly specialized software known as firmware used to

operate communications equipment made by Cobham Plc, the Harris Corporation, EchoStar Corp's Hughes Network Systems, Iridium Communications Inc., and Japan Radio Co. Ltd). In theory, a hacker could use a plane's onboard Wi-Fi signal or in-flight entertainment (IFE) system to hack into its avionics equipment, potentially disrupting or modifying satellite communications, which could interfere with the aircraft's navigation and safety systems.

Despite the sporadic attempts of Hackers' groups simulating attacks in laboratories around the world, the study found no documented evidence that existing aviation air-to-ground digital links have been subject to cyber-attack testing, i.e., improper access, denial of service (DoS), corrupted data packets, over-sized data packets, repeated identical messages, etc. The exception is the terminal wireless local area network unit (TWLU) Internet-based service.

A recent flight re-routing of more than 200 flights over Los Angeles International Airport (LAX) occurred due to a military aircraft transmitting a previously untested message as it prepared to enter commercial airspace, transitioning from military visual flying rules into commercial airspace rules. Additionally, after more than 20 years in service, Société Internationale de Télécommunications Aéronautiques (SITA) has verified that VHF Data Link Mode (VDL2) in Europe has developed an Aircraft Communications Addressing and Reporting System (ACARS) over Aviation VHF Link Control (AVLC) (AOA) no communication (NO COMM) condition on the aircraft, if data packets are not acknowledged. The NO COMM condition is believed to be caused by the increasing load on VDL2 links as Eurocontrol upgrades its capabilities. These two recent events demonstrate the need for additional air-to-grade link testing to stress the link and protocols, and evaluate them for cyber-attack induced failures.

The study did not find any existing cyber security testbeds for the testing of aircraft for cyber threats and vulnerabilities. Existing systems with airframers and their suppliers are highly proprietary, and not available or open to cyber security research or development. Thus, it is highly recommended that the FAA develop such simulators and testbeds; they are critical in supporting the full development of secure NextGEN, air traffic, management systems.

Another priority should be the development of guidance to ensure that airframers and their suppliers perform adequate cyber penetration testing on their aircraft. Testing must occur during the development, manufacturing, and maintenance involving any onboard network. Airframes and suppliers must ensure that their design is adequate, and that no inadvertent connectivity is created during the manufacturing or maintenance of the aircraft.

Finally, the vulnerabilities created during aircraft design and manufacture (1 and 2 above), are not easily studied by the FAA; however, the FAA should embark on the creation of a suite of cyber security policy guidance for industry to address the mitigation of threats created by these vulnerabilities.

Given the recent discoveries of advanced persistent threats in United States (US) industry, and the insertion of backdoors in commercial products, these threats have the potential to affect entire aircraft model lines. Thus, protection of aircraft design and manufacture should be a priority. Aircraft design and software modules need protection from unauthorized changes for both new aircraft and design modifications to existing aircraft or systems. Digitally signed software modules should be validated prior to loading to aircraft. For aircraft flight critical components, audits should be required of their supply chain.

1. INTRODUCTION

1.1 PURPOSE

The purpose of this study is to provide the FAA Tech Center with an initial analysis of cyber threats to the current generation of e-Enabled or connected aircraft, and to provide prioritized recommendations for follow-on research and industry guidance. Additionally, the study identifies common threats to legacy, current, and the next generation of aircraft.

1.2 BACKGROUND

The evolution of technology in aviation has been a growing trend since aviation's start in the early 19th century. Today's growing need for additional and improved aviation efficiency and safety has led manufacturing companies to develop and introduce new and more sophisticated solutions to better serve the industry. These solutions are very broad in type, and range from composite materials to new instrumentation for flight management and revolutionary aircraft wireless networks.

The adoption of new technology has led to the current generation of e-Enabled airplanes: aircraft that can participate as an intelligent node in a global information network. e-Enabled airplanes include advanced, highly integrated communications, navigation, and flight control systems for automated functionalities, e.g., global positioning systems (GPS) for navigation wireless sensors, onboard aircraft servers, extensive IFE systems, passenger Internet via satellite communications (SATCOM) or 3/4G technology, cell phone connectivity, numerous versions of the EFB, extensive portable electronic maintenance equipment, remote Internet access for electronic maintenance, aircraft health monitoring (AHM) systems, and radio frequency identification (RFID) tags for maintenance. Further, increasing time-to-market and cost reduction pressures have led to the dramatic proliferation of commercial off-the-shelf (COTS) components within aircraft.

Unfortunately, there are no regulations or safety policies addressing these problems effectively. Nonetheless, airlines should be aware of these vulnerabilities and adopt the necessary measures to protect their various networks and systems. This report provides high-level results on the investigation that MSAG conducted to assess the main building blocks for these aircraft domains.

1.2.1 Aircraft Architecture

Aircraft architecture varies from original equipment manufacturer (OEM) to OEM, and integrates several subsystems within the four virtual domains. The ARINC Airlines Electronic Engineering Committee (AEEC) Aircraft Data Networks (ADN) subcommittee developed a reference architecture figure (figure 1), which has found acceptance in the aeronautical community.

Its development was specific to facilitating the discussion on the various types of Internet protocol (IP) networks onboard today's aircraft, in addition to distinguishing those networks responsible for the continued safe flight of the aircraft found in the aircraft control domain (ACD). Figure 1 illustrates the different components and their relative functions in each of the aircraft domains.

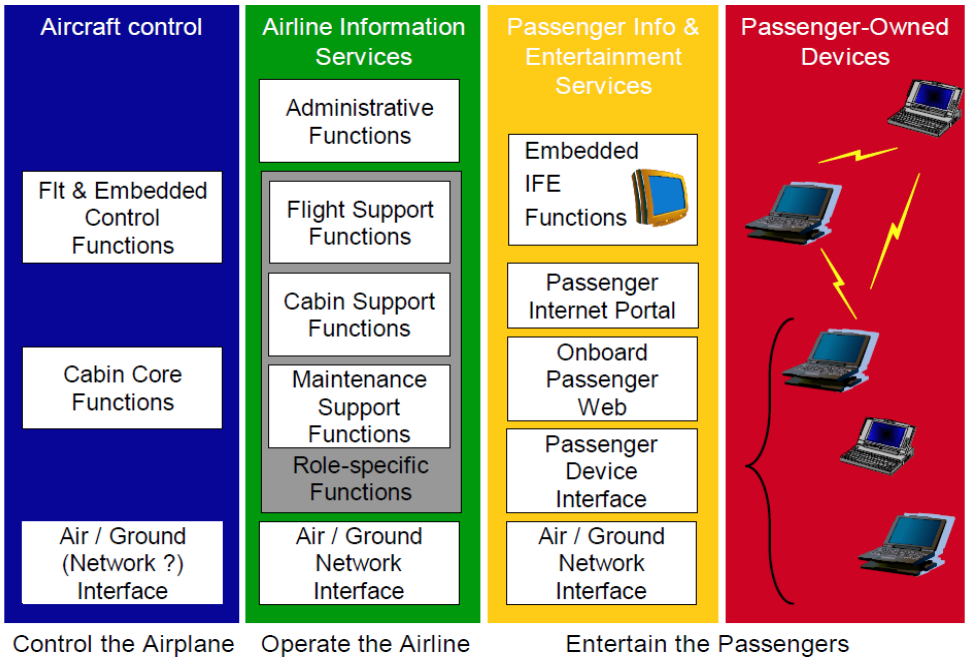

FIGURE 1. AIRCRAFT DOMAINS

Terrestrial IP-network-COTS technologies are used in the development of the majority of IP networks onboard the aircraft. In comparison with the life of the aircraft, IFE systems have a relatively short life cycle and enjoy the opportunity to use state-of-the-art COTS network technologies. Figure 2 provides a high-level architecture of how these three logical domains are connected. It classifies the types of communication links among the different modules in each domain, for a generic aircraft.

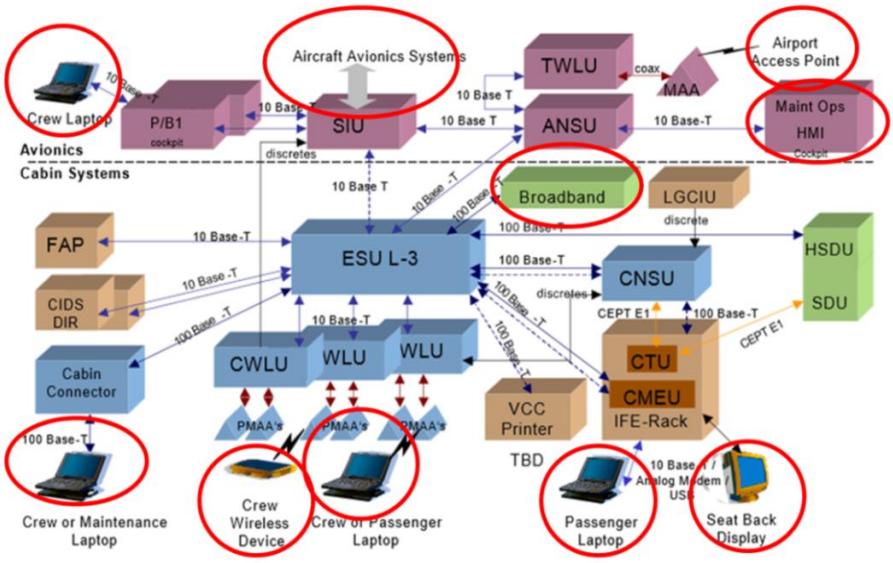

FIGURE 2. AIRCRAFT ARCHITECTURE
AND AREAS OF CYBER CONCERN

The above aircraft architecture includes other subsystems that are equally important and provide risk to an aircraft network. High-risk aircraft systems, processes, and components, possibly considered as multiple instantiations of this model, include:

Field Loadable Software

- Thousands of aircraft use field loadable software for electronic parts via wireless connectivity
- Increased implementation of wireless networks for new applications
- Use of cyclic redundancy checks (CRCs) as the validation of the software part

User Modifiable Software (UMS)

- Electronic checklists
- Navigation data bases
- EFB user loadable/modifiable software applications

AMI

These are software configurations that an airline can customize to suit its needs. They include the ability to create or customize items such as airplane condition monitoring function (ACMF) reports and functions, aircraft server network configurations, TWLU link authentications, and aircraft public key infrastructure (PKI) certificates.

Ground Based Software Tool (GBST)

The GBST compiles, tests, and releases AMIs for loading into the aircraft systems.

COTS Devices

- Over 95 percent of electronic components used in aircraft today are COTS-based.
- Microprocessors
- General purpose integrated circuits

Integrated Modular Avionics (IMA) Systems

- Consists of numerous applications of differing failure classifications
- Backplanes, high-speed, bi-directional, data buses/switches can connect to an unlimited number of aircraft systems
- Most IMA systems use a common avionics full duplex Ethernet (AFDX) network, based on IP technologies.

EFB Systems

- Exchanges large volumes of operational information between aircraft and airline operations' centers
- Contain airline custom applications for airline operations support
- Electronic checklists
- Aircraft fault analysis trees

- Under consideration as an initial point for aircraft access to system-wide Information Management (SWIM) (AAtS)
- Most EFB systems have Internet access, at least at the gate, via the TWLU or 3/4G.

Wireless Systems

- Pass aircraft systems control information and commands
- Pass aircraft system information
- Pass aircraft health information

2. AIRCRAFT CLASSIFICATIONS

2.1 LEGACY AIRCRAFT GENERATION

Legacy aircraft do not possess any onboard networks with Internet access. The portable electronic maintenance aids and loadable software systems used in their maintenance may be connected to the Internet during use, or to receive maintenance or software part updates.

2.2 CURRENT GENERATION (CONNECTED A/C)

Current generation aircraft have Internet capability either built into them, as do the B-787 or A-380, or by retrofitting with the antennas, servers, and Internet connectivity necessary to provide service. Both the B-787 and A-380 have core AFDX networks that are accessible in maintenance mode from their Internet service. Legacy aircraft can move into the current generation if their upgrade includes items such as new communication links, EFBs installed, passenger and crew Internet services, or new data loaders utilizing smart technology.

2.3 NEW GENERATION

The new generation of aircraft will extend the use of Internet and COTS technology to include AAtS systems, ADS-B, and true next generation (NextGEN) digital guidance technology. They will make use of technologies introducing further cyber security challenges such as virtualized LRUs and systems to reduce weight and power by the sharing of processors, memory, and storage. Software defined radio (SDR) is another candidate technology having the potential to reduce the number of antennas required, as well as provide weight and power savings.

New AHM systems, black box streaming systems, and remote maintenance access systems incorporating Internet access are all either available or in development, and likely, will be usable on all generations of aircraft. Table 1 provides aircraft types within the Legacy and NextGEN architectures.

TABLE 1. AIRCRAFT TYPES WITHIN LEGACY AND NextGEN ARCHITECTURES

Legacy Aircraft Architecture	Current Generation of Connected A/C	New Generation of Aircraft w/NextGEN Simulation Capabilities
1. Architecture types • B-777 • A-320 • B-747 • Other 2. Messaging types • ACARS message • Gate clearances • Weight and	1. Virus detection 2. Authentication testing 3. DoS/bad data insertion 4. Loadable software protection 5. Firewall rules testing (pen testing) 6. Deep packet inspection 7. Encryption 8. Routing integrity (onboard	1. Unmanned aircraft system (UAS) integration (avoidance and collision, communication) simulation 2. Automatic dependent surveillance – broadcast (ADSB) simulation 3. AAtS simulation 4. NextGEN protocol

Legacy Aircraft Architecture	Current Generation of Connected A/C	New Generation of Aircraft w/NextGEN Simulation Capabilities
balance simulation 3. Loadable software • Legacy loaders • e-Enabled loaders (access control) • Integrity 4. Upgraded Legacy • Future air navigation system (FANS) • Controller-pilot data link communications (CPDLC) 5. Communication management unit (CMU)/Flight management system (FMS) 6. Aircraft condition monitoring system (ACMS) 7. Security test/Case insertion 8. Application and Tool support 9. National Air Space (NAS) replay 10. Maintenance tool interface (access control to aircraft systems) 11. Version checking loadable software 12. Scalable 13. Third-party simulator adapter	and offboard) 9. Domain name system (DNS) (impact on reliability) 10. IPV6 (inadvertent connection) 11. Enclave integrity (applied to the three aircraft domains) 12. EFB and onboard servers 13. Logging (ability to receive logs and check rules) 14. Illegal address detection and impact 15. Aircraft authentication: onboard and offboard	simulation 5. Virtual LRU security 6. Remote access to aircraft for electronic maintenance

3. AIRCRAFT ARCHITECTURE

3.1 AIRCRAFT CONTROL DOMAIN (ACD)

The ACD's predominant characteristics are its long life cycle – roughly equal to the airframe of more than 30 years – and the fact that systems within this domain are responsible for the continued safe flight of the aircraft, and are subject to regulatory agency certification. In this domain, important considerations are the safety aspects of networks, and that the interconnection of systems/devices is simple and understood by regulatory agencies.

In contrast to terrestrial network design, many ACD network, architecture design decisions are made to facilitate the safety analysis/certification process rather than to achieve extra performance. At the base of any aircraft architecture are communication links managed by buses, such as ARINC 429.

Since the 1970's, ARINC 429 digital buses have been used to connect digital equipment, with ARINC 629 coming in the 1990's, and AFDX being introduced with the current generation of aircraft. These 429 and 629 buses consist of a single transmitter connected to one or more receivers—allowing a piece of equipment to transmit to several others. The AFDX bus is based on Internet and Ethernet, but is highly customized for aircraft to improve its deterministic abilities. Generally, devices transit onto an AFDX segment, with all devices hearing the transmission and selecting only those they are configured to receive. In IP terms, this is multicasting. Basic sets of data parameters are multicast to the receiving equipment at rates up to 100 Mb/sec. The connection of equipment and functions is deterministic, and can be readily determined using the wiring interconnect documents.

In the 1980's and 1990's, the 429 and 629 system buses were developed using various shared media in time-division multiple access (TDMA) schemes. Data could be received by the equipment when transmitted in their appropriate time slot, and for any equipment needing the data—notoriously known as a multicast paradigm. In this case, pre-stored data tables described which equipment and functions received the data of others. Table 2 provides a summary of the different buses utilized in aircrafts.

TABLE 2. BUS TYPES USED IN AIRCRAFT

Bus Technology	ARINC 429	1553B	ARINC 629	Ethernet	AFDX
Bandwidth (HZ)	100KB	1MB	2MB	1GB	100MB
Communication Mode	Simplex	Half duplex	Half duplex	Half duplex	Full duplex
Number of terminals	20	32	120	Unlimited	Don't limit (in theory)
Walk-the-line difficulty	Complex	Medium	Medium	Simple	Simple
Cost price	Low	Higher	High	Low	Low
Reliability	Higher	Higher	Higher	Low	High

Today, it should not be surprising to see multicast remain the dominant form of communication in the ACD on the AFDX bus. For IP type networks such as AFDX, user datagram protocol (UDP) is the natural choice for multicasting. In addition, since networks within the ACD are reliable in a bit-error-rate sense, trivial file transfer protocol (TFTP) over UDP can be used for the relatively small file transfers necessary in this domain; simple network management protocol (SNMP) over UDP is also supported.

Similar to the simplicity of UDP, IP can be simplified. For example, in a closed ACD network, IP packet sizes can be controlled to the point where IP fragmentation and reassembly are not necessary. A lengthy discussion on the simplification of IP networks within the ACD took place during ARINC AEEC ADN Subcommittee meetings where the concept of compliant and profiled IP networks emerged. ARINC PP664 Part 3 documents these concepts. Compliant networks are compliant to Institute of Electrical and Electronics Engineers (IEEE) RFCs. A profiled network is an allowed simplification for networks in the ACD in order to ease the safety-of-flight analysis and certification. The Internet Protocol (IP) networks in the ACD can simply avoid the use of transmission control protocol (TCP) and use UDP. SNMP uses UDP, and TFTP over UDP can be used for relatively small file transfers.

The ARINC 429 medium is responsible for the information transfer between avionics systems and primary flight displays (PFDs) (aircraft interface), and between the PFDs themselves (cross-link interface). The ARINC 429 data bus will be in accordance with the requirements defined in the ARINC 429P1 standard.

3.2 CURRENT ONBOARD COMMUNICATIONS BUSES

The ARINC 429 medium contains sixteen ARINC 429 input channels and eight ARINC 429 output channels. The following devices from the aircraft system can communicate with the PFD through the ARINC 429 medium:

- Air data computer (ADC)
- Communications management unit (CMU)
- Inertial reference system (IRS)
- Standby flight display (SFD) (acts as secondary ADC and IRS)
- Barometric correction
- Cross PFD
- Flight management system (FMS)
- Mission computer (MC)
- Radar altimeter
- Traffic and collision alert device (TCAD)
- Very high frequency (VHF) omnidirectional range/Instrument landing system (VOR/ILS)
- Distance measuring equipment (DME)
- Tactical air navigation (TACAN)

- Flight director/Auto pilot (FD/AP)
- Remote I/O concentrator (RIOC)

ARINC 629 was introduced in May 1995 and is currently used on the Boeing 777, Airbus A-330, and A-340 aircraft. The ARINC 629 bus is a true data bus in that it operates as a multiple-source, multiple sink system. That is, each terminal can transmit data to, and receive data from, every other terminal on the data bus. This allows much more freedom in the exchange of data between units in the avionics system. The true data bus topology is much more flexible in physically accepting units on the data bus. Another attraction of ARINC 629 is its ability to accommodate up to 128 terminals on a data bus, though in practice, the amount of data bus traffic controls the number of terminals used. It supports a data rate of 2Mbps, represents a significant improvement in configuration and communications capabilities over 429, and has similar devices with which it communicates.

ARINC 664 is typically called AFDX, despite being an Airbus patented term. It is in use on the B-787, A-350, and A-380. AFDX adopted concepts (token bucket) from the telecom standard asynchronous transfer mode (ATM), to fix the shortcomings of IEEE 802.3 Ethernet by adding key elements from ATM to those already found in Ethernet, and constraining the specification of various options. Therefore, a highly reliable Full-Duplex deterministic network is created providing guaranteed bandwidth and quality of service (QoS). Full-Duplex Ethernet eliminates the possibility of transmission collisions. The network's design prioritizes all critical traffic using QoS policies so that delivery, latency, and jitter are guaranteed to be within set parameters.

A highly intelligent switch common to the AFDX network is able to buffer transmission and reception packets. Utilizing twisted pair or fiber optic cables, full-duplex Ethernet uses two separate pairs or strands for transmitting and receiving data. AFDX extends standard Ethernet to provide high data integrity and deterministic timing allowing operation to 100 megabits per second. Further, use of a redundant pair of networks improves system integrity (although a VL (virtual link) may be configured to use one network or the other). It specifies interoperable functional elements at the following OSI reference model layers:

- Data link (MAC and VL addressing concept)
- Network (IP and ICMP)
- Transport (UDP and optionally TCP)
- Application (network) (Sampling, queuing, SAP, TFTP and SNMP)

The main elements of an AFDX network are:

- AFDX end systems
- AFDX switches
- AFDX links

It has a similar list of connected devices as the 429 and 629 buses, and typically transmits and receives in modes similar to multi-cast. Studies are underway to consider supporting gigabit or multi-gigabit modes, as well as the migration from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6). The ARINC 664 specification states that all aircraft using AFDX

have the same onboard network addressing plans. The vision is for AFDX to support increasing onboard traffic in next generation of aircraft.

Special conditions have been required for its use as it both connects more devices and communicates with onboard systems having offboard IP links. The link to AFDX and these systems is supposed to be inoperable without weight-on-wheels (WOW). Airbus uses a transmit only diode architecture to allow AFDX data, typically aircraft health, to those onboard systems during flight; the diode design prevents transmission onto the AFDX networks without WOW.

3.3 AIRCRAFT INFORMATION SERVICE (AIS)

The AIS domain provides air traffic control (ATC), airline administrative, and non-safety airline communications. Most communications to the ACD pass through this domain: software parts, data loading, AMIs, maintenance logs, engine monitoring, etc. This domain currently supports ACARS, FANS, VDL Mode 2, and CPDLC communications links. ACARS connectivity through these legacy links to an ATS provider does not require a security assessment.

In current generation aircraft domains, TWLU, SATCOM, and 3G/4G media are used to support IP communication links and EFBs. Using IP across these media types, results in a highly flexible, interoperable communications capability, especially to retrofit legacy aircraft with new technologies and communications. Currently, loadable software, EFB updates, navigation database updates, engine monitoring, etc., are transmittable or receivable via IP over the TWLU, 3G/4G links, or IP SATCOM.

The next generation of aircraft will include EFB interfaces and displays on the PFDs, ADS-B, and NextGEN ATC digital guidance in the AIS domain. In addition, expectations are that current ACARS, FANS, VDL Mode 2, and CPDLC will be accessible via SATCOM or 3G/4G IP links. This domain is also targeted to receive the AAtW applications to allow more digital communications between the pilots and controllers. Moreover, the addition of remote maintenance access is a likely addition to this domain in next generation aircraft.

ACARS, FANS, VDL Mode 2, CPDLC, and EFB connectivity to an airline's operations center should require a security assessment, if the information received by the aircraft systems can be written to the ACD. An example is flight plan information possibly transmitted from ground-based systems in an airline's operations center and written to the control display unit of a Flight Management Computer System.

3.4 PASSENGER INFORMATION AND ENTERTAINMENT SYSTEMS (PIES)

The PIES domain provides entertainment and communications (e.g., voice, Internet connectivity) directly to passengers. It is transitioning to a new term, passenger-owned devices (PODs). This domain will likely include cargo-embedded devices developed for customs, cargo tracking, and environmental and shock recording. A security assessment and Special Condition (SC) should be issued for any non-ATS providers' external network connected to the PIES domain having write access that is physically connected to the ACD, or shares communications links with the AIS or ACD domains. Devices shared between the AIS and PIES/POD domains require special attention. Discussions are ongoing about printers, scanner, and other crew systems that will likely support electronic passenger and baggage manifests, as well digital messaging between passengers and crew. Work is ongoing to provide access to all aircraft domains over a single

communications link. Currently, security assessments and SCs are not required for any non-ATS provider's external network connection to the PIES domain, if there is no write access or physical connection to the ACD.

3.5 RISK ANALYSIS

This section covers the primary areas of cyber risk to the model aircraft.

3.5.1 Design, Manufacture, and Maintenance

Cyber threats to aircraft actually begin with its design and manufacturing. Currently, most aircraft design processes have limited security built into them. During development, code is open and left unprotected on servers, possibly for weeks or months. This time period provides an opportunity for the insertion of malware or backdoors in the code. Another threat is the installation of malware or backdoors in the code via software tools such as configuration management or compilers. The same risk applies to the digital design process of the physical aircraft in the modification of its digital parts. The result is potentially shortening airframe life or reliability, as a competitive advantage. In both cases, more rigorous security requirements should be implemented to formally authorize both code checkouts for the model databases, and the daily digital signing of the code as an engineer completes work or checks the code back into the development model databases. These potential gaps in code/design security are even more concerning with the continuing rumors of corporations being infiltrated with what is known in cyber security as advanced persistent threats (APTs). With an APT, infiltrators may have had access for months, or even years, into the core of a corporation.

A similar threat exists with the issue of having trust in the aircraft supply chain. An aircraft is composed of tens of thousands of individual electronic components and systems from around the world. Thus, the insertion of malware or backdoors to the aircraft in one of these components or systems is not inconceivable. Recently, members of Congress were briefed on this threat by high-level national security staff, as there are concerns not just about commercial products but also about our military systems.

3.5.2 Loadable Software

Another potential path to aircraft is through the loadable software parts that manufacturers distribute with the aircraft, and may occasionally update. Figure 3 provides a high level of loadable software distribution.

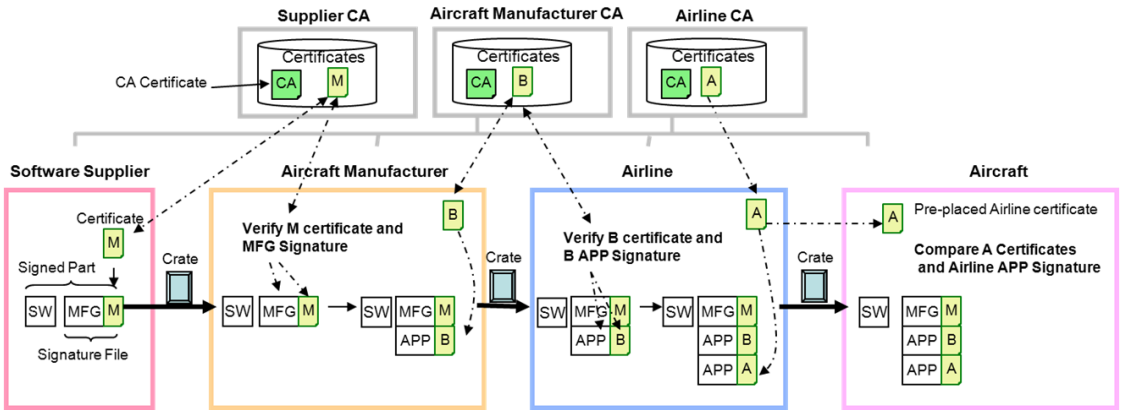

FIGURE 3. SOFTWARE END-TO-END DISTRIBUTION PROCESS

Although there is an increasing use of digitally signed parts by industry to ensure that the digital model or loadable software is not corrupted or altered before it is loaded, this practice holds largely to the current generation of e-Enabled aircraft. Distribution of legacy aircraft parts was via true floppy disk, and then diskettes. Typically, the airline copied data to servers for long-term storage, but with minimal security applied to server storage. This is further complicated as airlines have been updating older aircraft with floppy or diskette readers to use smart technologies like wireless interfaces, Bluetooth, Universal Serial Bus (USB) memory modules, or maintenance laptops. These new technologies introduce additional cyber risks that need examining, as they are smart devices as opposed to the purely digital recording floppy disk technology, which has no inherent capabilities to do anything but read or write data. Possible threat scenarios to sabotage aircraft include:

- **Asset Corruption** - The contents of distributed software can be altered or replaced (in an undetectable manner) to provoke early component failures, or even failure of flight critical systems. This type of corruption to airplane-loadable software is sometimes referred to as coherent corruption, emphasizing a distinction from random bit errors, which would generally render a software component unloadable. Airplane-generated data can be also corrupted to threaten airplane safety, e.g., by altering safety-related reports.
- **Software Misconfiguration** - In order to wreak havoc, a mismatch between the airplane's intended and actual configuration can be provoked by preventing delivery of software, deleting software, or injecting inappropriate software during distribution.
- **Asset Diversion** - Software can be diverted to an unsuitable recipient to provoke accidents, e.g., by disturbing the execution of other software at that destination.
- **Asset Staleness** - The revocation and update of software that needs to be changed for safety reasons can be blocked and delayed, thus impeding the distribution processes.

Business threats include:

- **Asset Unavailability** - Assets can be rendered inaccessible or unusable, for example by jamming asset distribution to disrupt airplane service.
- **Late Detection** - Assets can intentionally be corrupted so that the tampering is detected late enough for the airplane to be put out of service. For example, when tampering of

software is not detected during distribution from ground systems to airplane, but is only detected upon final load at the destination LRU in the receiving airplane. Software corruption that is detectable by an LRU, or whose installation renders the LRU non-functional, is distinct from that referred to above as coherent corruption.

- **False Alarm** - Assets can be tampered with to cause economic damage from misleading safety concerns. In particular, corruption of configuration reports might cause an airplane to appear as if incorrectly configured, creating unwarranted flight delays from the misleading safety concerns.
- **Repudiation** - Any entity in the software loading system could deny having performed security-relevant actions, e.g., deny having distributed or received some software.

The number of loadable software in newer aircraft varies from model to model and are exponentially increasing in presence. Figure 4 represents the number of field loadable software by aircraft.

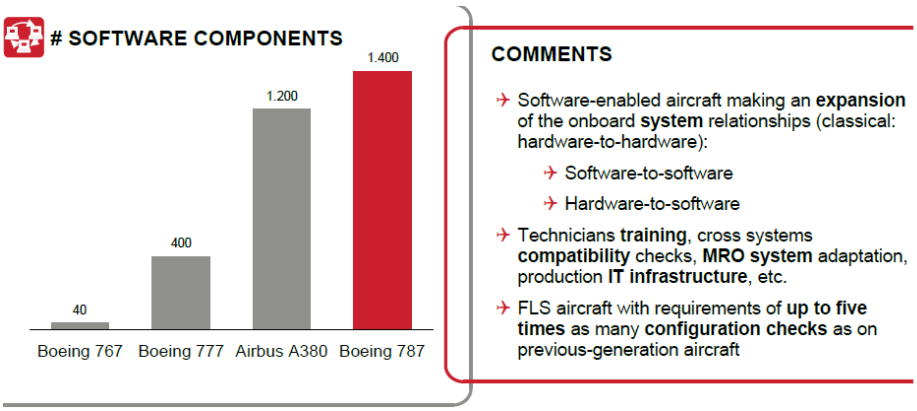

FIGURE 4. FIELD LOADABLE SOFTWARE BY AIRCRAFT

Table 3 provides a list of know software currently in use in Boeing's aircrafts. All airframers have a similar list of loadable software parts.

TABLE 3. FIELD LOADABLE SOFTWARE IN BOEING AIRCRAFT

Loadable Software	Airplane(s)
Advanced cabin entertainment and service system (ACESS)	747
Air data inertial reference unit (ADIRU)	777
Air data module (ADM)	777
Air supply and cabin pressure controllers (ASCPC)	777
Airborne vibration monitor (AVM)	777
Aircraft communications addressing and reporting system (ACARS)	737-700/-800/-900, 747, 757, 767
Airfoil and cowl ice protection system (ACIPS)	777
Airplane condition monitoring system (ACMS/printer)	747

Loadable Software	Airplane(s)
Airplane condition monitoring system (ACMS) (flight data recorder system) (FDRS)	767
Airplane information management system (AIMS)	737-700/-800/-900, 747, 757, 767, 777
ARINC signal gateway (ASG)	777
Automatic flight director computer (autopilot) (AFDC)	777
Auxiliary power unit (APU)	737-700/-800/-900
Auxiliary power unit controller (APUC)	777
Backup electrical power system (BEPS)	777
Bridge router (BROUTER)	777
Bus power control unit (BPCU)	777
Cabin management system (CMS)	747, 777
Cabin telecommunication unit (CTU)	737-700/-800/-900, 757
Cabin temperature controller (CTC)	777
Cargo smoke detector system (CSDS)	777
Central maintenance computer system (CMCS)	747
Common display system (CDS)	737-700/-800/-900
Control display unit (CDU)	777
Digital flight data acquisition unit (DFDAU)	737-700/-800/-900, 757
Duct leak overheat detection system (DLODS)	777
Electrical load management system (ELMS)	777
Electronic engine control (EEC)	777
Electronic flight instrument system (EFIS)	757, 767
Engine data interface unit (EDIU)	777
Engine indication and crew alerting system (EICAS)	757, 767
Enhanced ground proximity warning system (EGPWS)	737-700/-800/-900, 757, 767
Environmental control system miscellaneous card (ECSMC)	777
Flap/slat electronics unit (FSEU)	777
Flight control computer (FCC)	737-700/-800/-900, 757
Flight deck printer (PRINTER)	777
Flight management computer (FMC)	737-700/-800/-900, 767
Flight management computer system (FMCS)	747, 757

Loadable Software	Airplane(s)
Flight management computer/ control display unit (FMC/CDU)	737-700/-800/-900
Fuel quantity indicating system (FQIS)	777
Generator control unit (GCU)	777
Global positioning system sensor unit (GPSSU)	777
Hydraulic interface module (HYDIM)	777
Integrated display system (IDS)	747
Interactive videodisk system (IVS)	747, 767
Interactive videodisk system (video) (IVS)	767
Maintenance access terminal (MAT)	777
Portable maintenance access terminal (PMAT)	777
Primary flight computer (PFC)	777
Satellite communication system (SATCOM)	737-700/ -800/-900, 747, 757, 767
Satellite communication system data unit (SDU)	777
Standby attitude air data reference unit (SAARU)	777
Traffic alert and collision	737-700/-800/-900
Avoidance system (TCAS)	777
Warning electronics unit (WEU)	777
Weight on wheels (WOW)	777

3.5.3 Airline Modifiable Parts

Another avenue of similar potential risk is the increasing use of AMI parts that airlines either purchase or create themselves, such as navigational databases. In some cases, the AMIs update aircraft, cyber security protection such as the IP tables, firewall rules, or PKI certificates which represent other avenues of risk.

3.5.4 Internet Access Points

Wireless access points (WAP) in the aircraft, the TWLU at the gate, IP over SATCOM or 3/4G links facilitate communication between onboard systems, as well as with the offboard infrastructures of ATC or airlines (aircraft-to-infrastructure (A2I)) and another aircraft (aircraft-to-aircraft communications or (A2A)). COTS and wireless solutions can substantially reduce onboard equipment maintenance overhead, as well as system weight. These facts, and achievable enhancements in information delivery, availability, usage, and management, make the e-Enabled airplane a promising, cost-effective basis for improvements in flight safety, schedule predictability, maintenance, operational efficiencies, and other areas. However, all of these access points introduce cyber risks to the aircraft.

3.5.5 Aircraft Electronic Portable Maintenance Aids

Commercial aircraft systems are routinely electronically interrogated through portable maintenance computers connected to special ports in the aircraft systems, and by other trusted users including pilots using mobile computers to support aircraft operations. Generally based on standard COTS operating systems (OS), these computers are subject to the same cyber vulnerabilities as exist in their base OS. Generally connected to commercial Internet services, these maintenance computers are often completely unprotected, both from receiving updates of aircraft software and navigation databases, as well as to the downloading of aircraft maintenance information collected while the unit is connected to the aircraft.

3.5.6 Multi-domain Use of Air-to-Ground Links

As air-to-ground communications grow in importance, not only for airline operational/passenger Internet and voice access, but also for air traffic management and airline operational communications, standards and advanced design work are underway for multi-domain use communications links. The development of multi-use links is a necessity, as they reduce both power and weight requirements, as well as interference between links and antenna placement proximity restrictions. Nevertheless, these activities introduce a risk of breach between the domains; risks to be addressed by the implementation of proper security controls to separate domain communications.

3.5.7 Remote Maintenance Access

In this same line of planning, IFE vendors are designing new systems with remote electronic maintenance capabilities, whether at the terminal or in flight. Airlines have already requested that airframe manufacturers design aircraft electronic maintenance systems allowing remote access to the aircraft at the gate, via either the TWLU or hardwired Gatelink connections. The FAA faces challenges to develop accurate oversight procedures, guidance, and regulations to assure the safety of air transportation in the US, through the introduction of these solutions.

3.5.8 Aircraft Network Domains

As technology advances, the obvious spinoff is the increased efficiency and productivity of aircraft, airlines, and the air traffic system (ATS). The venue is e-Enabled aircraft that automatically connects and interacts in real-time with airlines and service providers' ground-based stations and ATS. New generation e-Enabled aircraft (A-380, A-350, B-787, C-Series, and others, including a few business jets) have their systems linked to ground stations in real-time. Data uploads and downloads drive these operational efficiencies.

e-Enabled aircraft have unique networking, computing, security, certification, and physical operating requirements that render integration a daunting challenge. With the release of e-Enabled aircraft, the use of IT infrastructure onboard the airplanes has progressed significantly over the last few years. The expectation is that the use of COTS solutions will continue at a fast pace. e-Enablement means the architecture of new systems for aircraft will be composed of several connected networks. The four major domains currently distinguished are ACD, AIS, aircraft virtualization, and aircraft communications links, elaborated on in the following sections.

3.5.8.1 ACD (or sometimes still referred to as the ATC Domain)

The ACD's design is to be a closed domain for safety-related control and navigation systems. It is the most critical domain, and primarily encompasses the systems that control the operation of the aircraft. Communication with it from other domains or maintenance equipment is prohibited during flight; it may only send data during flight and may not receive data requests or acknowledgements. Currently, the ACD uses only high frequency (HF) or VHF communications; however, work is underway to certify Internet over SATCOM and 3/4G links for the safety of flight communications.

The ACD is divided into two sub-domains: flight and embedded control system sub-domain, where the aircraft is controlled from the flight deck and cabin core sub-domain, which provides environmental functions dedicated to cabin operations, such as environmental control, passenger address, smoke detection, etc.

3.5.8.2 AIS Domain (or sometimes still referred to as the AOC Domain)

The airline information services domain (AISD) provides general-purpose routing, computing, data storage and communications services for non-essential applications. The AISD may provide services and connectivity between independent aircraft domains such as avionics, in-flight entertainment, cabin distribution and any connected off-board networks. The AISD is subdivided into two sub-domains:

1) Administrative sub-domain, which provides operational and airline administrative information to both the flight deck and cabin; and

2) Passenger support sub-domain, which provides information to support the passengers.

The AIS domain's definition is predominately for airline business and administrative support. Gatelink operates through the terminal wireless unit (TWU), and is only accessible to the AOC or for aircraft maintenance personal; currently, passengers cannot access TWLU links. As EFBs have been deployed as part of this domain, 3/4G wireless connectivity is often available at the gate for use by passengers, service, maintenance, and flight crew. EFBs, onboard aircraft servers, WAP, crew tablets, and pilot cell phones are also part of this AIS Domain.

3.5.8.3 Passenger-Owned Devices Domain (PODD), and the Passenger Information and Entertainment Services (PIES) Domain.

The PODD includes only those devices that passengers may bring on board and may connect to the PIES. Until they connect via the PIES, the PODs should be considered external to the airplane network regardless of their connection to one another or directly off-aircraft to ground systems without involving the airplane network.

The (PIES) domain includes any device or function of a device that provides services to passengers. Beyond traditional IFE systems, it may also include passenger device connectivity systems, passenger flight information systems (PFIS), broadband television or connectivity systems, seat actuator or message system and controls, and functions of an information server device providing services to passengers via the IFE devices.

The PODD and PIES are also private domains, and prohibited from any communications with other domains at all times; however, there is pressure to allow passenger access to crew devices, such as printers. These devices are in the public domain, and are essentially comprised of PODs, which may interface to IFE or Internet-connected systems provided by the aircraft operator, or directly to each other. The private domains of the AOC and PIES/PODD rely on new types of connectivity, such as a cabin wireless network connected to SATCOM or 3/4G link provider for access to the Internet.

These new network architectures present cyber security risks and potential vulnerabilities that require addressing. The major cyber concern is that any wired or wireless devices used within the aircraft, including the personal devices used by passengers, can provide entry points into the aircraft onboard networks allowing inadvertent, unauthorized access to the ACD and AISD through errors in design, manufacture, or maintenance. The consequences of these activities could cause intentional or unintentional corruption of data and applications residing on the onboard servers that are critical to the safe operations of aircraft.

It is conceivable that this type of inadvertent access could expose systems to being halted or misdirected, or to insert fake system faults into the aircraft maintenance databases, potentially grounding an aircraft until maintenance personnel can clear it for takeoff. This represents a huge cost for the airline. Domain network links that could inadvertently be misconfigured or mis-wired creating unauthorized connectivity between the domains is yet another basic risk during manufacture or maintenance of the aircraft.

A new risk developing in this area is due to the growth of personal privacy electronic shields. The shields' design is to provide some protection to the individual from electronic recording and video monitoring systems, and operate on numerous, wireless spectrums. These units can be the size of a small phone. With the introduction of small software defined radio (SDR) units, it will be possible for a single unit to operate in multiple spectrums. The risk from these units is their inadvertent jamming of aircraft wireless control and communications systems. The aircraft of the current generation utilize multiple onboard wireless systems in several different spectrums.

3.5.8.4 Aircraft Virtualization

The next generation of aircraft will add even more cyber security complexities to aviation. Aircraft manufacturers are exploring new technologies such as virtualization for onboard servers and components to improve aircraft architectures. The coming years will foresee a drastic increase in the use of virtualized systems and LRUs, and more common bus/network traffic, with even more sharing of individual unit memory and processes between these virtualized components to reduce weight and wiring.

All of these elements introduce completely new cyber vulnerabilities to aircraft. This is especially true as these systems are far more likely to be vulnerable to the introduction of malware and the installation of backdoors as they are based on COTS technologies similar to laptops or tablets. It is critical to ensure that the prioritization of the applications and LRU functions cannot be circumvented by DoS type attacks that could steal processor cycles or memory from priority tasks, or block communications by flooding the network with data.

3.5.8.5 Aircraft Communications Links

As the FAA develops its NextGEN air traffic management system, along with Eurocontrol's SESAR capabilities, aircraft will increasingly rely on digital direction from navigation service providers around the globe. Also on the horizon are the use of ADS-B and likely, a similar system for UAVs to pinpoint them to general and commercial aviation. This means that the number of aviation communication protocols and services will drastically increase, requiring additional testing to ensure that recent events such as the LAX en route automation modernization (ERAM) service disruption are caught much earlier.

Further, despite being in service for years and the increasing link data loading of the Voice Data Link 2 (VDL2) link with both AOA and Aeronautical Telecommunications Network (ATN) traffic, an issue with apparently lost data packets has caused serious concern as some vendor CMUs can go to a NO COMM state, confirmed by SITA in June 2014. If the ground does not acknowledge AOA downlinks, it can lead to an AOA NO COMM situation; however, ATN is not affected and continues to flow well. When AOA uplinks resume, but are no longer acknowledged by avionics (suspected due to the AOA NO COMM condition), the AOA NO COMM situation would last on that same link as long as ATN is connected. The condition disappears only if the link hands off to another station, which could be lengthy.

In today's cyber world, these new link types, especially those based on Internet technologies, need to be more fully tested. Measures must be taken to ensure that inadvertent errors such as these two examples do not exist, and that aircraft are not susceptible to cyber risks, such as DoS attacks that insert fake or corrupted data, direct penetration, or spoofing over the links.

3.5.9 Onboard Aircraft Control and Communications Wireless Systems

Wireless systems are used to control cabin systems such as lighting, seat audio, galley systems, etc., and to communicate aircraft system health data and RFID tags information. As mentioned in the PIES/PODDs section, these systems may suffer interference or be jammed inadvertently by personal privacy electronic shields. Thus, a risk assessment of the system's criticality and ability to function during jamming, whether inadvertent or malicious, should be part of required certification testing.

4. RECOMMENDATIONS

The design and implementation of onboard aircraft networks is highly proprietary, and limited information by both the airframers and their suppliers is only available to the FAA under very tight NDAs prohibiting its publication or disclosure in any form. This study focused on the current generation of e-Enabled aircraft using publicly available information on the B-787 and A-380, as base models for the current generation of e-Enabled or connected aircraft. Both aircraft are built around ARINC standards for aircraft networks and connectivity. It includes, as part of the study, the base ARINC standards for air data networks.

The study presents the general threats that exist in the current generation a connected aircraft model with multiple network domains onboard, terminal wireless connectivity, Internet connectivity for passengers and crew, LRUs shared between aircraft domains, loadable software, EFBs, etc. It also covers the cyber threats that exist during the aircraft design process and through the supply chain during its manufacture.

Study results show that the aircraft is most vulnerable to five types of threats:

1. Manipulation of the aircraft loadable software parts and the AMI components.
2. Inadvertent or deliberate interconnection of the aircraft domains during manufacture, maintenance, or modifications.
3. Unexpected vulnerabilities to attacks directed at aircraft offboard communications links or onboard wireless aircraft control and internal communications systems, including common attacks to penetrate the aircraft domains and denial of communications services.
4. Manipulation of the aircraft digital design and software components during design, or upgrades.
5. Insertion of backdoors or malware into aircraft electronic components or systems via the supply chain during manufacture.

The manipulation of aircraft loadable software parts and AMIs should receive the highest priority for further study and research, as these threats exist to virtually all commercial aviation aircraft as they are used in legacy aircraft, current generation aircraft. Moreover, even more software parts and loadable virtualized systems will exist in the next generation of new aircraft. Follow-on work should create credible demonstrations of the threats to these and recommended countermeasures to protect the loadable software and AMIs. Initiating research should also be initiated on the specific vulnerabilities that virtualized systems and LRUs will present in order to be prepared to write cyber guidelines for them.

The vulnerability of the existing aircraft communications link to unexpected cyber-attacks and conditions during link design should also be a high priority research task. The study found no documented evidence, except for the TWLU Internet-based service, which the existing aviation air-to-ground digital links have been subject to cyber-attack testing (i.e., improper access, DoS, corrupted data packets, over-sized data packets, repeated identical messages, etc.). Also, recent flight re-routing of more than 200 flights over LAX occurred due to a military aircraft beginning to transmit untested as it prepared to enter commercial airspace. Additionally, after more than 20 years in service, SITA has verified that VDL2 in Europe has developed an AOA NO COMM condition on the aircraft if data packets are not acknowledged. It is believed that this is caused

by the increasing load on VDL2 links as Eurocontrol upgrades its capabilities. These two recent events demonstrate the need for additional air-to-grade link testing to stress the link and protocols and to evaluate them for cyber-attack induced failures.

In addition, a priority should be to develop guidance to ensure that the airframers, and their suppliers, perform adequate cyber penetration testing on their aircraft during development, manufacturing, and any maintenance involving any onboard network, ensuring that their design is adequate and no inadvertent connectivity was created during the manufacturing or maintenance of the aircraft.

Finally the vulnerabilities present during the aircraft design and manufacture (numbers 4 and 5) are not easily studied by the FAA; however, a suite of expected cyber security policy guidance should to be provided by the FAA to industry to mitigate this threat. However, given the recent discoveries of advanced persistent threats in US industry and the insertion of backdoors in commercial products, they have the potential to affect entire aircraft model lines, thus their protection should be a priority. Aircraft design and software modules should be cyber protected from the initiation of the study of new aircraft models or modifications to existing aircraft and digitally signed modules should be delivered with the aircraft. For aircraft flight critical components, supply chain audits should be required.

5. CONCLUSIONS

A significant risk exists across legacy, current, and next/new generation aircraft; loadable software modules, and airline modifiable information components. Current commercial aviation standards only require their protection with a 32-bit cyclic redundancy check. This technology was developed in the 1960's and 1970's with the advent of the 32-bit processors, and was designed only to detect random flips of one to a few bits. Attacks on how to modify the code while preserving the CRC value have been published on the Internet for over a decade. Thus, these models are vulnerable to a cyber-attack.

The A-350 and A-380 do require validation of the modules digital signature before it can be loaded; this practice should be required for all generations of aircraft. While retrofitting legacy and current aircraft to use stronger protections may not be viable, regulations and continued airworthiness guidelines should be developed that would ensure the digital protection of these modules from creation through installation on the aircraft. Several technologies exist, such as digital signatures, to provide this protection within the ground infrastructure of the manufacturer and airline during creation, distribution, and as a final check before loading into the aircraft.

The FAA should develop demonstrations of cyber risks to loadable software and AMIs to share with the industry for training. The Agency should also develop guidance for aircraft cyber security certification processes to include mandatory penetration testing of aircraft networks modeling the FSA FedRAMP process for testing cloud storage, and services for US Government use. The study endorses developing guidance ensuring the audit of the electronic supply chain. This measure safeguards against malware or backdoors insertion into the aircraft through the installation of tampered electronic component or systems.

Another significant cyber risk to commercial aviation exists in the current generation of aircraft represented by the B-787 and A-380 aircraft models. The risk is that aircraft domains may be inadvertently interconnected during design, manufacture, or maintenance or be given improper access to offboard communications systems. Penetration testing of the aircraft, before delivery and after any maintenance involving the aircraft's networks, substantially reduces risk, even if maintenance occurs on only one domain. Penetration testing to ensure that the aircraft onboard networks will not allow any communication to the ACD during flight is also critical. This type of threat may also exist on legacy aircraft retrofitted with Internet access, or aircraft where there are EFBs installed or used that have any Internet connectivity.

Finally, the study found no existing aircraft simulators capable of testing aviation aircraft-to-ground communication links for cyber threat. Their existence is not publicly disclosed, nor are they likely to be available for FAA or industry cyber-risk research, or cyber security development due to the potential disclosure of proprietary system designs. The need for this type of aircraft simulator, specifically designed for cyber risk analysis and testing is critical, especially as a proliferation of new types of aircraft communication links are added to commercial aircraft (i.e., IP over SATCOM, ADSB, GPS, Worldwide Interoperability for Microwave Access, Inc. [WiMAX], etc.). Thus, it is strongly recommended that the FAA develop an aircraft cyber security simulation and test bed capable of testing the communication links for both network layer cyber risks and media links exploitation.