DOT/FAA/TC-14/28

Office of Aviation Research
and Development
Washington, DC 20591

Perform an Industry Survey

Date: 08/01/2014

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 (DOT)
Federal Aviation Administration (FAA)

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-14/28		

4. Title and Subtitle	5. Report Date
Perform an Industry Survey	July, 31st 2014
	6. Performing Organization Code NA
7. Author(s) Terry Davis, Dennis Glatting, Eric Jacobs, and Luigi Valentini	8. Performing Organization Report No. Deliverable 0001
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- June 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 partners that can represent the laboratory, and explores potential collaboration with the FAA, if the work is relevant.

Short summary of report

This report provides a comprehensive assessment of the various aviation simulator capabilities within private and public organizations, and government agencies. The report identifies the different types of simulators in the US territory, addresses how they are used, and their possibilities to be used for advanced research in aviation. The report also provides an extended review of COTS solutions and university research, with respect to aviation and simulation.

17. Key Words	18. Distribution Statement
Aircraft security; simulation, modeling, safety	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	3
1.1 PURPOSE	3
1.2 BACKGROUND	3
2. SIMULATOR BASELINE SCORING SYSTEM	5
2.1 EVALUATION APPROACH	7
2.2 IDENTIFY TECHNOLOGIES IN USE	7
2.2.1 TRAINING SIMULATORS	7
2.2.2 ENGINEERING SIMULATORS	35
2.3 GOVERNMENT LABORATORIES	38
2.3.1 FAA CIS LABORATORIES	38
2.3.2 AVIATION COMMUNICATION TESTING LABORATORY	38
2.3.3 NAVY	39
2.3.4 NASA	39
2.3.5 UNITED STATES AIR FORCE (USAF)	40
2.4 UNIVERSITY LABORATORIES	40
2.4.1 VIRGINIA POLYTECH INSTITUTE AND STATE UNIVERSITY	40
2.4.2 THE INSTITUTE OF AVIATION AT THE UNIVERSITY OF ILLINOIS	41
2.4.3 UNIVERSITY OF TORONTO INSTITUTE FOR AEROSPACE STUDIES (UTIAS)	41
2.4.4 WEST VIRGINIA UNIVERSITY (WVU)	42
2.4.5 UNIVERSITY OF MARYLAND EASTERN SHORE (UMES)	43
2.4.6 THE UNIVERSITY OF TENNESSEE SPACE INSTITUTE (UTSI)	44
2.4.7 WICHITA STATE UNIVERSITY (WSU)	44
2.4.8 EMBRY-RIDDLE AERONAUTICAL UNIVERSITY (ERAU)	45
2.4.9 UNIVERSITY OF NORTH DAKOTA (UND)	45
2.5 PRIVATE LABORATORIES	45

2.6 SIMULATOR INTEGRABILITY WITH FAA REQUIREMENTS 46
2.6.1 APPROACH TO COLLABORATION 46
2.6.2 ISSUES 48
2.6.3 CHALLENGES 49
2.6.4 RISKS 50
3. AIRCRAFT CYBER ANALYSIS AND THREAT SIMULATOR (ACATS) PHYSICAL VIRTUALIZATION, AND CYBER TESTING SYSTEM ARCHITECTURE 52
3.1 PURPOSE 52
3.2 INFRASTRUCTURE TIER 53
3.2.1 VIRTUALIZATION STORAGE 55
3.2.2 ATTACKING HASHES 56
3.2.3 VERSIONING 57
3.2.4 INFORMATION SHARING 57
3.2.5 SPACE REQUIREMENTS SUMMARY 57
3.3 ADDITIONAL INFRASTRUCTURE TIER DETAIL 58
3.4 INTERFACING TIER 59
3.5 EQUIPMENT TIER 59
3.6 VIRTUAL AND OTHER SERVICES 60
3.7 TEST EQUIPMENT GROUP AND HARDWARE IN THE LOOP INTERFACING 60
3.7.1 BEAGLE BOARDS 62
3.8 TEST SUPPORT EQUIPMENT GROUP 62
3.9 THREAT ASSESSMENT EQUIPMENT GROUP 64
3.10 SIMULATION EQUIPMENT GROUP 64
3.11 DEVELOPMENT GROUP 64
3.12 SOFTWARE 64
3.13 DECOMPOSITION 65
4. CONCLUSIONS 66
5. REFERENCES 67

APPENDICES

A— VENDOR WEB ADDRESSES
B— REFERENCES

LIST OF FIGURES

Figure	Page
FIGURE 1. MODELS OF COLLABORATION	47
FIGURE 2. ACATS MACRO VIEW	53
FIGURE 3. INFRASTRUCTURE TIER	53
FIGURE 4. ROUTING INSIDE/OUTSIDE	54
FIGURE 5. LOCAL STORAGE STACK	55
FIGURE 6. INFRASTRUCTURE TIER NETWORKING AND STORAGE	59
FIGURE 7. HIGH-LEVEL DEPICTION OF EQUIPMENT TIER	60
FIGURE 8. BEAGLE BOARD EXPANDERS	61
FIGURE 9. MIGRATION FROM THE PHYSICAL TO THE VIRTUAL	62
FIGURE 10. TEST SUPPORT GROUP	63

LIST OF TABLES

Table	Page
TABLE 1. AIRCRAFT TYPES WITHIN LEGACY AND NEXTGEN ARCHITECTURES	5
TABLE 2. TRAINING SIMULATORS	8
TABLE 3. COTS FLIGHT SIMULATOR PRODUCTS	36
TABLE 4. FAA CONCEPT AND INTEGRATION (CSI) LABORATORIES	38
TABLE 5. AVIATION COMMUNICATION TESTING LABORATORy	39
TABLE 6. NAWCAD	39
TABLE 7. NASA	40
TABLE 8. WPAFB	40
TABLE 9. VIRGINIA POLYTECH INSTITUTE AND STATE UNIVERSITY	40
TABLE 10. INSTITUTE OF AVIATION AT THE UNIVERSITY OF ILLINOIS	41
TABLE 11. UTIAS	42
TABLE 12. WVU	42
TABLE 13. UMES	43
TABLE 14. UTSI	44
TABLE 15. WSU	44
TABLE 16. ERAU	45
TABLE 17. UND	45
TABLE 18. COLLABORATION MODELS AND DESCRIPTIONS	46
TABLE 19. CHALLENGES TO COLLABORATION	49
TABLE 20. COLLABORATION RISKS	50

LIST OF ACRONYMS

AATD	Advanced Aviation Training Device
AAtS	Aircraft Access to System-Wide Information Management
ACs	Advisory Circulars
ACARS	Aircraft Communications Addressing and Reporting System
ACATS	Aircraft Cyber Analysis and Threat Simulator
ACATT	Aircraft Cyber Analysis and Threat Test-bed
ACD	Aircraft Control Domain
ACMS	Aircraft Condition Monitoring System
AD	Active Directory
ADB-S	Automatic Dependent Surveillance-Broadcast
AFDX	Avionics Full-Duplex
AFMC	Air Force Material Command
AFRL	Air Force Research Labs
AND	Aircraft Data Network
ANSS	Aircraft Network Security Simulator
ARNIC	Aeronautical Radio Incorporated
ASC	Aeronautical Systems Center
ATC	Air Traffic Control
ATG	Approval Test Guide
B-ATDs	Basic-Aviation Training Devices
BSD	Berkeley Software Distribution
CANbus	Controlled Area Network
CDs	Compact Discs
CGAR	Center of Excellence of General Aviation Research
CMU	Communication Management Unit
COTS	Commercial-off-the-shelf
CPDLC	Controller-Pilot Data Link Communications
CSF	Cockpit Simulation Facility
CVSRF	Crew-Vehicle Systems Research Facility
DNS	Domain Name System

DOF	Degree of Freedom
DoS	Denial of Service
EFB	Electronic Flight Bag
ERAU	Embry-Riddle Aeronautical University
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FMS	Flight Management System
FTDs	Flight Training Devices
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFR	Instrument Flight Rules
HF	High frequency
HLA	High-level architecture
IMA	Integrated Modular Avionics
I/O	Input/output
IP	Issue Papers
iSCSI	Internet Small Computer System Interface
ISO	International Standards Organization
JND	Just-noticeable-difference
LRUs	Line Replaceable Units
LUN	Logical Unit Number
MFD	Multi-function Display
MITM	Man-in-the-middle
NAS	National Air Space
NASA	National Aeronautical
NAWCAD	Naval Air Warfare Center, Aircraft Division
NFV	Network Function Virtualization
NTLM	NT LAN Manager
OI	Operational Improvements
OSI	Open Systems Interconnection
PCATDs	Personal Computer-based Aviation Training Devices
PIES	Passenger Information Entertainment Services

PODS	Passenger Owned Devices (PODS)
POS	Position Reference
PSK	Pre-shared keys
R&D	Research and Development
RDT&E	Research, Development, Test, and Evaluation
RF	Radio frequency
SC	Special Conditions
SDR	Software Define Radio
SLAs	Service Level Agreements
SWIM	System-Wide Information Management
TC	Type Certificate
TCP/IP	Transmission Control Protocol/Internet Protocol
TTP	Time-triggered protocol
TWLU	Terminal wireless LAN unit
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicles
UND	University of North Dakota
UPRT	Upset Prevention and Recovery Training
US	United States
USAF	United States Air Force
USB	Universal Serial Bus
UTIAS	University of Toronto Institute for Aerospace Studies
UTSI	University of Tennessee Space Institute
UUT	Units Under Test
WPAFB	Wright Patterson Air Force Base
WVU	West Virginia University

EXECUTIVE SUMMARY

Physical risks to aircraft safety change over time as both society and technology evolve. This inevitability forces changes in aircraft design, operation, and maintenance, in order to maintain acceptable risk levels. 9/11 resulted in re-analysis of physical risks to aircraft and a new requirement to retrofit aircraft with stronger cockpit doors. "Bomb location" studies have initiated new operational requirements for tighter control of aircraft access on the tarmac, and different types of in-service inspections are required for new composite hulls and parts. Cyber risks, like physical risks, transform and escalate with changes in society and technology.

Aircraft cyber threats and vulnerabilities have been increasing rapidly due to the proliferation of "loadable software", wireless technology, commercial-off-the-shelf (COTS) components, widely used communication protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP), and the integration of systems that were historically stand-alone. Early mitigation of the potential risk to "loadable software" modules required that the code carried a standard aviation 32-bit checksum, similar to those used to validate aircraft systems' communications against random bit errors. To address risk, requirements dictated that the loadable software media went through a defined "chain of custody" through isolated systems to ensure that unauthorized persons did not have access. Available technology of the time rendered floppy disks, diskettes, and compact discs (CDs) as "neutral media". These technologies had no inherent processing capabilities; they were the digital equivalent of "printed media".

Both technology and society have evolved significantly over the last decade, as have operating costs pressures. All of these variables affect cyber risks to aircraft. Loadable software is now installed via "smart" Universal Serial Bus (USB) system (memory sticks), specialized "maintenance" laptops, wired and wireless "private" networks, and even the Internet. With the advent of faster computers, software is now available that can re-write stored "loadable software" without changing the checksums. Finally, aviation has "connected" or "e-Enabled" aircraft that communicate wirelessly across private and public networks. Soon, these aircraft will be receiving advanced "next generation" navigation commands from "air navigation service providers" directly to the aircraft's guidance and control systems. Cyber risks to aircraft and the potential of compromised safety have metamorphosed to being a much greater presence than even a decade ago. Minimal effort is devoted to the simulation and replication of these attacks. Organizations have predominantly used simulator systems to train students in aircraft operations and to simulate the interaction between human and machines.

A decade ago, the risks to aircraft from a deliberate attack were completely "physical"; a decade from today, the threat will largely be "cyber". An example of the changing nature of cyber threats is that a recent, single cyber-attack on a United States (US) municipality's financial systems exceeded the total amount of money taken in that state's 250 armed bank robberies, the previous year.

In a decade, NextGEN aircraft guidance will be the norm; we will likely share the skies with commercial Unmanned Aircraft Systems (UAS), and aircraft will have remote maintenance performed on their electronic and software cores. We are an "electronic society" today. Aviation is rapidly moving in this direction, because of accelerating competitive and economic pressure,

and as an opportunity to increase safety. Thus, cyber security risk evaluation and mitigation must become part of the design and operational use strategies implemented by aircraft manufacturers, industry vendors, and aircraft operators.

In order to maintain the highest standards for aircraft safety, the Federal Aviation Administration's (FAA) regulations, policy and guidance, along with industry practices, must evolve. Evaluating aircraft systems and ATG communications for their cyber security risk should be part of the standard certification process. The need exists for the use of "baseline systems that mimic a generic aircraft network and communication's infrastructure" to allow advanced research and proofs–of-concept.

Evaluating cyber risks must be part of the basic validation of technologies in use in aircrafts. In all cases, cyber risk evaluations must ensure that the process maintains its ability to provide the certainty of its testing and validation requirements while still maintaining timeliness in the certification process.

Summary Findings

Our research analysis led us to an interesting and concerning finding that of the all simulators identified in this report, very few are involved in any aircraft, cyber security research. In both public and private sectors, investing in simulators is done to satisfy requirements for aircraft design, certification, continuous training, studies on human factors, advanced research on environmental stress, and aircraft operation (90%).

Although there are several commercial products and solutions for aircraft simulators, cyber security modeling and simulation are not major concerns for most operators and private organizations. Modeling and simulation predominantly apply to airframers and their major suppliers. These simulators are highly proprietary and not available to the FAA. So far, only academic papers reference aircraft cyber security testing, with no actual working simulators in either government or academia with significant cyber security research or testing capabilities.

Our vision for the FAA is to be able to start with limited, defined, cyber testing capabilities focused on near term risks but with the goal of having an advanced virtual simulation at development's end that can provide cyber threat analysis and testing. Thus, we recommend that the FAA initially utilize parts of open source flight simulators, and some purchased simulator software and hardware, to begin the development of cyber security research and testing capabilities with the FAA's Tech Center. The cyber threat simulation will require three to five years to reach maturity. At that time, anticipation is that close to 90% of the threat simulator will be virtualized and capable of being "cloud-based".

A "cloud-based" threat simulator will provide the most capable platform for collaborative research and development (R&D) with other agencies, academia, and industry, as a readily shared resource. A cloud-based model enables replication of the entire model. Distributing the replicated model for use by others would not affect the FAA's research capabilities. The model will also have the capability to interchangeably insert new, or updated, component versions for development or specific threat/model/functionality testing. We envision a configuration tool allowing engineers to create custom, independent models utilizing the components and versions for their specific research or testing.

1. INTRODUCTION

1.1 PURPOSE

The purpose of this task is to develop a comprehensive assessment of the various aviation simulator capabilities within private and public organizations, and government agencies. In performing the assessment, we classified simulators and activities based on the organization type (government, commercial, and universities). For the most relevant sites, we identified key information. This assessment is part of a larger scale effort aimed at identifying capabilities, architectures, integrability, and collaboration/sharing efforts among these organizations and the FAA.

The report is to provide the FAA a broader analysis of the different aircraft simulators on US soil for utilization in advanced research, especially in the area of cyber security of the ATG communications and basic aircraft systems. Our report provides a comparison rubric to simplify the categorization of simulators facilitating the easy recognition of sites and organizations of interest. It presents comparison matrices aimed at identifying simulator types and relevant characteristics of potential interest to the FAA, academia, and industry to clarify differences.

This assessment is part of a larger scale effort aimed at identifying capabilities, architectures, integrability, and collaboration/sharing efforts among these organizations and the FAA. At the base of this research is the FAA's need to develop plans and collaborative agreements for the development of an Aircraft Network Security Simulator (ANSS) at the Cockpit Simulation Facility (CSF) of the William J. Hughes Technical Center. The ANSS is an advanced framework as required by the Aviation Research Division in support of FAA studies of aircraft, network, cyber security vulnerabilities, and the effects of mitigation methods to establish airworthiness, continued airworthiness, and aircraft, operation, cyber security standards.

ANSS's basis for initial development is the ARINC 429 bus and ARINC-664 aircraft data network (ADN) specifications. It will be capable of interfacing with other types of simulators, network systems, either airborne or land-/satellite-based (wired/wireless), as well as other types of internal/external connectivity currently deployed and/or developed. ARINC 664 Part 7, often referred to as Avionics Full-Duplex Switched Ethernet (AFDX) (actually an Airbus patented implementation of Part7), ARINC 629, and controller area network (CANBus) capabilities expect to be added during the system development, as they are prioritized in the work.

This model will also serve as the FAA's basis to move into the research and testing of new approaching technologies that include "virtualized" Line Replaceable Units (LRUs), Software Defined Radio (SDR), Network Function Virtualization (NFV), and virtualized bus adapters. Over the next decade, these technologies will become a reality in aircraft, especially Unmanned Aerial Vehicles (UAVs), as they replace physical units with virtualized components that significantly reduce weight, wiring, and overall power consumption.

1.2 BACKGROUND

A lack of common certification standards exists in aircraft certification for the design and operation of communication networks and protocols. Currently, Type Certificate (TC) Special

Conditions (SC) and Issue Papers (IP), and Advisory Circulars (ACs) address incorporating existing network standards and COTS components, and other novel and innovative components into modern aircraft.

Modern aircraft are fitted or being retrofitted with COTS digital communication systems that directly or indirectly, connect to external networks, some of which are publicly accessible or share public interfaces. The private connections and protocols used are either adapted or direct implementations of standard protocols; therefore, they share common cyber-security threats. As the transmission and reception of digital information from air to ground and even air-to-air increases, the risk posed to aircraft safety also increases.

As digital data link channels evolve in speed and bandwidth, so too will its application from simple messaging to tactical operations, and strategic management. Information regarding flight operations and dispatching, crew operations, and maintenance data, currently routinely sent from the ground to the aircraft, will become more complex and possibly share interfaces with other non-flight related content (e.g., Position Reference (POS) and Passenger Information Entertainment Services (PIES)). Therefore, studying and understanding the systemic risks these and other technologies present to airworthiness and continued airworthiness of aircraft need, is prudent.

Avionic components are now communicating on Ethernet-based ADNs. The protocols used are deterministic and utilize elements of the Open Systems Interconnection (OSI) model (International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 7498-1) and a modified Institute of Electrical and Electronics Engineers (IEEE) 802.3 Ethernet protocol at the Media Access Control sub-layer. By adapting existing standards, it is possible to use COTS network components with modified network switches and end-systems. Along with Integrated Modular Avionics (IMA) and ADNs, using deterministic Ethernet and other real-time protocols like TTP (time-triggered protocol) allows modern aircraft to distribute the processing of safety critical elements within the Aircraft Control Domain (ACD). Currently, ACD systems with varying levels of criticality are either physically or logically isolated from external networks.

The lack of common certification standards for the design and operation of these systems is problematic in that without a clear, reliable, set of evaluation criteria, the potential for systemic security threats to work their way into designs exists. Furthermore, without common criteria, suitable assessment of potential security treats on aircraft safety is at best, ad hoc. Therefore, a means of defining and testing system designs and security concepts is necessary to ensure aircraft safety.

Today, the FAA does not have the capability to evaluate in-depth, cyber security concerns on aircraft systems, to simulate patterns of attack including manipulation of ATG communications messages, or to assess the security robustness of avionic systems. Equally, many aviation simulators focus on specific testing and are not broad enough to accommodate full testing and analysis. To mitigate these challenges, the FAA has launched an R&D project aimed to identify the different components and relationships ultimately, to develop a functional cyber simulator.

2. SIMULATOR BASELINE SCORING SYSTEM

The project's approach followed a structured and process driven methodology, leading to the creation of an evaluation baseline and scoring system for each of the reviewed simulators. The logic behind this approach was to review and score every simulator fairly for a variety of elements of interest to the FAA. We classified the simulators under two distinct types of aircraft architectures: legacy aircraft architectures, and the new generation of e-Enabled aircraft. Simulators built under a legacy aircraft category undergo evaluation for their affinity with the following:

- specific aircraft manufacturer's architectures (i.e., Boeing 747, 777, Airbus 320);
- the types of supported messaging;
- the ability to upload software;
- any upgraded legacy systems;
- the types of flight management systems;
- the ability to support security tests, tools and application integration;
- maintenance interfaces;
- ability to integrate with the National Air Space (NAS);
- scalability to accommodate new components; and,
- the ability to communicate with other simulators.

Table 1 outlines the types of aircraft classified within the two architectures used to evaluate simulators. **Note**: Capabilities are additive.

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 • Aircraft Communications Addressing and Reporting System (ACARS) Message • Gate clearances • Weight and	1. Virus detection 2. Authentication testing 3. Denial of service (DoS)/bad data insertion 4. Loadable s/w protection 5. Firewall rules testing (pen testing) 6. Deep packet inspection 7. Encryption 8. Routing integrity (on & off board) 9. DNS (impact on reliability)	1. UAS integration (avoidance and collision, communication) simulation) 2. Automatic Dependent Surveillance-Broadcast (ADB-S) simulation 3. Aircraft Access to System-Wide Information Management (SWIM) (AAtS) simulation 4. NextGen protocol simulation 5. Virtual LRU security

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) Aircraft Condition Monitoring System (ACMS) 6. Security Test/Case insertion 7. Application and Tool support 8. NAS 9. Maintenance tool interface (access control to aircraft systems) 10. Version checking loadable software 11. Scalable 12.Third party simulator	10. IPV6 (inadvertent connection) 11. Enclave integrity (applied to the 3 aircraft domains) 12. Electronic Flight Bags (EFB) & onboard servers 13. Logging (ability to receive logs and check rules) 14. Illegal address detection and impact 15. Aircraft authentication: onboard and offboard 16. Wireless for non-critical control and data recording systems.	6. Combined virtualized systems that utilize a common physical resources: process, comm, memory, etc. 7. Remote access to aircraft for electronic maintenance 8. Increased use of wireless and conductive communication's technologies. 9. Use of "control signaling and data acquisition over aircraft power wiring".

Legacy Aircraft Architecture	Current Generation of "Connected A/C"	New Generation of Aircraft w/NextGen Simulation Capabilities
adapter		

2.1 EVALUATION APPROACH

The MSAG Team performed extensive research on simulators for both commercial use and military application. Our approach is based on a precise review of each of the simulators used (research or training), the type of activities performed at the simulator, identification of the components used (virtual solutions or real components), any reference(s) to security and safety, the type of aircraft simulated, and the ability to simulate NextGen functions. We also identified simulator manufacturers and inquired as to their ability to replicate connectivity to flying instruments, the aircraft at the terminal and in-flight, and use of mobile support devices such as EFB and MOR aircraft diagnostic systems.

2.2 IDENTIFY TECHNOLOGIES IN USE

2.2.1 TRAINING SIMULATORS

The MSAG Team identified over 300 simulators providing training capabilities and limited research. Table 2 lists simulators, their location, the type of aircraft, and the manufacturing company. Among simulators, few have been used for generic research (FedEx Simulator) such as medical, and/or human factor analysis.

TABLE 2. TRAINING SIMULATORS

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
ABX Air	Wilmington, OH	767-200	CF6-80A	L-3 Link UK	FFS	SP3/4w	FAA	LC	1997
ABX Air	Wilmington, OH	DC-8-62	JT3D	L-3 Link UK	FTD	SP1/4w	FAA	LB	1990
ABX Air	Wilmington, OH	DC-9-30	JT8D	Singer-Link /Opinicus	FFS	ESIG3350/180	FAA	LC	2003
AIMS Flight Training Center	Greeley, CO Beech	1900D	PT6A	TDI	FFS	RasterFlite/4w	FAA	LC	2001
Alaska Airlines	Seattle, WA	737-300/400		L-3 Link UK	FFS	SPX200/4w	FAA	LC	1992
Alaska Airlines	Seattle, WA	737-700		L-3 Link UK	FTD				1999
Alaska Airlines	Seattle, WA	737-800		CAE	FFS	Tropos 6000		LD	2013
Alaska Airlines	Seattle, WA	CRJ700	CF34-8C1	CAE	FFS	Maxvue+/180	FAA	LD	2001
Alaska Airlines	Seattle, WA	CRJ700	GE CF34-8C1	CAE	FFS	Maxvue+	FAA	LD	2001
American Airlines Flight Academy	Dallas/Fort Worth, TX	727-200	JT8D	CAE	FFS	SP3T/4w	FAA	LD	1981
American Airlines Flight Academy	Dallas/Fort Worth, TX	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	2001
American Airlines Flight Academy	Dallas/Fort Worth, TX	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	2000
American Airlines Flight Academy	Dallas/Fort Worth, TX	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	1998
American Airlines	Dallas/Fort	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	1998

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Flight Academy	Worth, TX								
American Airlines Flight Academy	Dallas/Fort Worth, TX	737NG		CAE	FFS 7000	Tropos	FAA	LD	2009
American Airlines Flight Academy	Dallas/Fort Worth, TX	757-200	RB211	CAE	FFS	ESIG3350/180	FAA	LD	2001
American Airlines Flight Academy	Dallas/Fort Worth, TX	757-200	RB211	CAE	FFS	SPX500HT/150	FAA	LD	1990
American Airlines Flight Academy	Dallas/Fort Worth, TX	757-200	RB211	CAE	FFS	SPX200T/150	FAA	LC	1992
American Airlines Flight Academy	Dallas/Fort Worth, TX	767-200		L-3 Link UK	FFS	SP1/4w	FAA	LC	1982
American Airlines Flight Academy	Dallas/Fort Worth, TX	767-200	CF6-80A	CAE	FFS	ESIG3350/4w	FAA	LD	1987
American Airlines Flight Academy	Dallas/Fort Worth, TX	767-300ER	CF6-80C2	CAE	FFS	ESIG3350/180	FAA	LD	1999
American Airlines Flight Academy	Dallas/Fort Worth, TX	777-200	Trent 892	CAE	FFS	ESIG3350/180	FAA	LD	2000
American Airlines Flight Academy	Dallas/Fort Worth, TX	777-200	Trent 892	CAE	FFS	ESIG3350/180	FAA	LD	1999
American Airlines Flight Academy	Dallas/Fort Worth, TX	777-200	Trent 892	CAE	FFS	ESIG3350/180	FAA	LD	2001
American Airlines Flight Academy	Dallas/Fort Worth, TX	ATR 42-300	PW127E	CAE	FFS	SPX200T/4w	FAA	LC	1991
American Airlines	Dallas/Fort	ERJ-145	AE3007A	CAE	FFS	ESIG3350/180	FAA	LD	1998

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Flight Academy	Worth, TX								
American Airlines Flight Academy	Dallas/Fort Worth, TX	ERJ-145	AE3007A	CAE	FFS	ESIG3350/180	FAA	LD	2000
American Airlines Flight Academy	Dallas/Fort Worth, TX Fokker	100		CAE	FFS		FAA	LD	
American Airlines Flight Academy	Dallas/Fort Worth, TX Fokker	100	Tay 650-15	CAE	FFS	SPX500HT/150	FAA	LD	1991
American Airlines Flight Academy	Dallas/Fort Worth, TX MD	82		CAE	FFS	Image IIIT/4w	FAA	LC	1988
American Airlines Flight Academy	Dallas/Fort Worth, TX MD	82	JT8D	CAE	FFS	ESIG3350/4w	FAA	LD	1988
American Airlines Flight Academy	Dallas/Fort Worth, TX MD	82	JT8D	CAE	FFS	ESIG3350/4w	FAA	LD	1991
American Airlines Flight Academy	Dallas/Fort Worth, TX MD	82	JT8D	CAE	FFS	ESIG3350/4w	FAA	LD	1985
American Airlines Flight Academy	Dallas/Fort Worth, TX MD	82	JT8D	CAE	FFS	ESIG3350/4w	FAA	LD	1985
American Airlines	Dallas/Fort Worth, TX	82	JT8D	CAE	FFS	SPX500HT/150	FAA	LD	1985

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Flight Academy	MD								
Atlas Air	Miami, FL	747-200	CF6-50	L-3 Link UK	FFS	SPX250/150	FAA	LC	1980
Atlas Air	Miami, FL	747-200F		L-3 Link UK	FFS	SP1T/4w	FAA	LC	1981
Atlas Air	Miami, FL	747-400	CF6-80C2	CAE	FFS	Tropos 6000/Lcos	FAA	LC	1990
Boeing Flight Services (Atlanta)	Atlanta, GA	717-200	BR715-A1/C1	CAE	FFS	Vital VIII	FAA	LD	2001
Boeing Flight Services (Atlanta)	Atlanta, GA	717-200	BR715-A1/C1	CAE	FFS	EP8000	FAA	LD	2001
Boeing Flight Services (Atlanta)	Atlanta, GA	737-700/800	CFM56-7B	FSI	FFS	EP8000	FAA	LD	2001
Boeing Flight Services (Miami)	Miami, FL	737-300	CFM56-3C1	FSI	FFS	EP1000/4W	FAA	LC	1989
Boeing Flight Services (Miami)	Miami, FL	737-700/800	CFM56-7B	CAE	FFS	ESIG3800/180	FAA	LD	2001
Boeing Flight Services (Miami)	Miami, FL	737-700/800	CFM56-7B	FSI	FFS	Vital VIII /180	FAA	LD	2001
Boeing Flight Services (Miami)	Miami, FL	737-800	CFM56-7B	CAE	FFS	EP1000CT	FAA	LD	2009
Boeing Flight Services (Miami)	Miami, FL	757/767	CF6-80C2, PW4060, RB211	CAE	FFS	Vital VIII	FAA	LD	2001
Boeing Flight Services (Miami)	Miami, FL	757-200	PW2037, RB211-534E4	FSI	FFS	EP1000CT	FAA	LC	1991
Boeing Flight Services	Miami, FL	767-300ER	PW4056	FSI	FFS	EP1000CT/4W	FAA	LC	1991

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
(Miami)									
Boeing Flight Services (Miami)	Miami, FL	777-300ER	GE90-115	FSI	FFS	EP1000CT	FAA	LD	1999
Boeing Flight Services (Miami)	Miami, FL	A320-200	CFM56-5B4 V2527-A5	L-3 Link UK	FFS	SP1T/4w	FAA	LC	1988
Boeing Flight Services (Miami)	Miami, FL	MD-11	CF6, PW4460	CAE	FFS	EP1000CT	FAA	LD	1990
Boeing Flight Services (Seattle)	Seattle, WA	717-200	BR715	FSI	FFS	Vital VIII	FAA	LD	1999
Boeing Flight Services (Seattle)	Seattle, WA	737-700/800	CFM56-7B	CAE	FFS	EP8000	FAA	LD	1997
Boeing Flight Services (Seattle)	Seattle, WA	737-700/800	CFM56-7B	CAE	FFS	EP8000	FAA	LD	1998
Boeing Flight Services (Seattle)	Seattle, WA	747-8/-400	CF6-80C2B1F	CAE	FFS	EP1000CT	FAA	CAAC ILC/LD	2009
Boeing Flight Services (Seattle)	Seattle, WA	767-300ER	CF6-80C2, PW4060	L-3 Link UK	FFS	EP1000CT	FAA	LC	1987
Boeing Flight Services (Seattle)	Seattle, WA	777-200ER/300ER	GE90-94, RR Trent 895, GE90-115	CAE	FFS	EP1000CT	FAA	CASS, HK CAD, EASA LD	2006
Boeing Flight Services (Seattle)	Seattle, WA	787	GE/RR	L-3 Link UK	FFS	EP1000CT	FAA	EASA, TC, DGAC-Chile ILC	2010

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Boeing Flight Services (Seattle)	Seattle, WA	787	GE/RR	L-3 Link UK	FFS	EP1000CT	FAA	EASA, TC, CAAC, DGAC-Chile ILC	2009
CAE Charlotte Training Centre (US Airways)	Charlotte, NC	CRJ100/ 200	CF34-3A1/3B1/8C1	CAE	FFS 7000	Maxvue+/180	FAA	LD	2004
CAE Charlotte Training Centre (US Airways)	Charlotte, NC	CRJ700/ 900	CF34-3A1/3B1/8C1	CAE	FFS 7000	Maxvue+/180	FAA	LD	2002
CAE Dallas Training Centre	Dallas/Fort Worth, TX	737NG	CFM56-7B	CAE	FFS 7000	Maxvue+/180	FAA	LD	2002
CAE Miami Training Centre (Airbus Training Centre)	Miami, FL	A320 family		CAE	FFS 7000	Tropos 6200			2012
CAE Miami Training Centre (Airbus Training Centre)	Miami, FL	A320 family	CF56-5B4	CAE	FFS 7000	ESIG3350/180	FAA, JAA	LD	2001
CAE Miami Training Centre (Airbus Training Centre)	Miami, FL	A320-200	CFM56-5A	CAE	FFS 7000	ESIG3350/180	FAA, JAA	LD	1999
CAE Phoenix Training Centre (Arizona State University)	Phoenix, AZ	CRJ700/ 900	CF34	CAE	FFS 7000	Maxvue+/180	FAA	LD	2002
CAE Phoenix Training Centre (Arizona State	Phoenix, AZ	ERJ-135/145	AE3007A	CAE	FFS 7000	Maxvue+/180	FAA	LD	2003

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
University)									
CAE Phoenix Training Centre (US Airways Training Center)	Phoenix, AZ	CRJ700/ 900	CF34	CAE	FFS 7000	Maxvue+/180	FAA	LD	2003
CAE San Francisco Training Centre	San Francisco, CA	A320 family		CAE	FFS 7000	Maxvue+/180	FAA	LD	2002
CAE/Alaska Airlines	Seattle, WA	737NG		L-3 Link UK	FFS	ESIG3800/180	HKCAD	LD	2001
CRM Airline Training Center	Phoenix, AZ	737-200A	JT8D-15A	GMI	FFS	Image II/4w	FAA	LC	1985
Delta Air Lines	Atlanta, GA	727-200	JT8D	CAE	FFS	SP1/4w	FAA	LC	1981
Delta Air Lines	Atlanta, GA	737-200	JT8D	CAE	FFS	ESIG3350/180	FAA	LD	1999
Delta Air Lines	Atlanta, GA	737-200	JT8D	L-3 Link UK	FFS	SP2/4w	FAA	LC	1983
Delta Air Lines	Atlanta, GA	737-200	JT8D	L-3 Link UK	FFS	SP3/150	FAA	LC	1983
Delta Air Lines	Atlanta, GA	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	2000
Delta Air Lines	Atlanta, GA	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	1998
Delta Air Lines	Atlanta, GA	737-800	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LD	1999
Delta Air Lines	Atlanta, GA	747-200	JT9D	Singer-Link	FFS	SP1/4w	FAA	LC	1982
Delta Air Lines	Atlanta, GA	747-200	JT9D-7R	Singer-Link/ ATCO	FFS	SPX250CT/150	FAA	LC	1990
Delta Air Lines	Atlanta, GA	747-400	PW4056	CAE	FFS	SPX500HT/150	FAA	LD	1989
Delta Air Lines	Atlanta, GA	747-400	PW4056	Singer-Link/NATCO	FFS	SPX250CT/150	FAA	LC	1990

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Delta Air Lines	Atlanta, GA	757-200	PW2037	CAE	FFS	ESIG3350/180	FAA	LC	1989
Delta Air Lines	Atlanta, GA	757-200	PW2037	CAE	FFS	ESIG3350/180	FAA	LC	1984
Delta Air Lines	Atlanta, GA	757-200	PW2037	L-3 Link UK	FFS	SPX550HT	FAA	LD	1992
Delta Air Lines	Atlanta, GA	757-200	PW2037	Link/Opinicus	FFS	SPX500/4w	FAA	LD	1985
Delta Air Lines	Atlanta, GA	757-200	PW2037	Singer-Link/NATCO	FFS	SPX500HT/150	FAA	LC	1990
Delta Air Lines	Atlanta, GA	757-200	PW2037/RB211	CAE	FFS	SPX250CT/4w	FAA	LC	1990
Delta Air Lines	Atlanta, GA	767-200	CF6-80A	CAE	FFS	ESIG3350/180	FAA	LC	1983
Delta Air Lines	Atlanta, GA	767-300	CF6-80C2	CAE	FFS	SPX550/150	FAA	LD	1991
Delta Air Lines	Atlanta, GA	767-300ER	CF6-80C2	CAE	FFS	SPX550HT/150	FAA	LD	1991
Delta Air Lines	Atlanta, GA	767-300ER	CF6-80C2, PW4060	CAE	FFS	ESIG3350/180	FAA	LD	2001
Delta Air Lines	Atlanta, GA	767-400ER	CF6-80C2, PW4060	CAE	FFS	ESIG3350/180	FAA	LC	1999
Delta Air Lines	Atlanta, GA	777		CAE	FFS	Tropos	FAA	LD	2008
Delta Air Lines	Atlanta, GA	777-200	Trent 892	CAE	FFS	ESIG3350/180	FAA	LD	1999
Delta Air Lines	Atlanta, GA	787-8		L-3 Link UK	FFS	EP1000CT/200		LD	2009
Delta Air Lines	Atlanta, GA	A320-200	CFM56-5A1	CAE	FFS	ESIG3350/180	FAA	LD	1998
Delta Air Lines	Atlanta, GA	A320-200	CFM56-5A1	L-3 Link UK	FFS	SPX500HT/150	FAA	LC	1990
Delta Air Lines	Atlanta, GA	A320-200	CFM56-5A1	Singer-Link/NATCO	FFS	SPX250CT/4w	FAA	LC	1990

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Delta Air Lines	Atlanta, GA	A320-200	CFM56-5A1	Singer-Link/NATCO	FFS	SPX250CT/150	FAA	LC	1991
Delta Air Lines	Atlanta, GA	A330/ A340	CF6-80E1 PW4168A, Trent 772B; CFM56-5C	CAE	FFS	Vital VIII	UK CAA	LD	2002
Delta Air Lines	Atlanta, GA	A330-300	PW4168A	L-3 Link UK	FFS	ESIG3350/180	FAA	LD	2003
Delta Air Lines	Atlanta, GA	DC-9-30	JT8D-15,7, 9	Link/Opinicus	FFS	ESIG3350/180	FAA	LD	1990
Delta Air Lines	Atlanta, GA	DC-9-30	JT8D-15,7, 9	Singer-Link/NATCO	FFS	SPX500HT/150	FAA	LD	1990
Delta Air Lines	Atlanta, GA	DC-9-30	JT8D-7/9A	CAE/Opinicus	FTD	SPX500/4w	FAA	LB	1975
Delta Air Lines	Atlanta, GA	DC-9-30	JT8D-9A	CAE/Opinicus	FFS	ESIG3350/4w	FAA	LC	1983
Delta Air Lines	Atlanta, GA	L1011-100/250	RB211-22B	CAE	FFS	SP1/4w	FAA	LC	1971
Delta Air Lines	Atlanta, GA	L1011-250	RB211-524B4	Singer-Link/ARI	FFS	SPX200/4w	FAA	LC	1971
Delta Air Lines	Atlanta, GA	MD-11	CF6-80C2, PW4060	CAE	FFS	SPX550HT/150	FAA	LD	1990
Delta Air Lines	Atlanta, GA	MD-11	CF6-80C2, PW4060	L-3 Link UK	FFS	SPX200/150	FAA	LC	1992
Delta Air Lines	Atlanta, GA	MD-88	JT8D	CAE	FFS	SPX550HT/150	FAA	LD	1991
Delta Air Lines	Atlanta, GA	MD-88	JT8D	CAE	FFS	SPX550HT/150	FAA	LC	1992
Delta Air Lines	Atlanta, GA	MD-88	JT8D	CAE	FFS	SPX550HT/150	FAA	LD	1990

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Delta Air Lines	Atlanta, GA	MD-88	JT8D	Singer-Link/BSC	FFS	SPX550HT/150	FAA	LD	1988
Delta Air Lines	Atlanta, GA	MD-90		CAE	FFS	SPX550HT/150	FAA	LD	1993
Embry-Riddle Aeronautical University	Prescott, AZ	727-100	JT8D	CAE		NVS/2w			1994
Embry-Riddle Aeronautical University	Prescott, AZ	727-100	JT8D	CAE		NVS/2w			1994
Embry-Riddle Aeronautical University	Prescott, AZ	MD-90	V2500	CAE	FFS	Maxvue/150	FAA	LD	1994
FAA	OK City, OK	727-200	JT8D	CAE	FFS	SP1T/6w	FAA	LC	1984
FAA	OK City, OK	737-800		CAE	FFS	Tropos/180	FAA	LD	2004
FAA	OK City, OK	A330/A340		CAE	FFS	Tropos 6000		LD	2008
FedEx	Anchorage, AK	MD-11F	CF6-80C2	CAE	FFS	EP1000CT/150	FAA	LD	1997
FedEx	Memphis, TN	727-2S2F	JT8D	L-3 Link UK	FFS	SPX550HT/150	FAA	LD	1987
FedEx	Memphis, TN	A300-600F	CF6-80C2	CAE	FFS	EP1000CT/150	FAA	LD	1993
FedEx	Memphis, TN	A300-600F	CF6-80C2	L-3 Link UK	FFS	EP1000CT/150	FAA	LD	1997
FedEx	Memphis, TN	A310-200	CF6-80A	CAE	FFS	EP1000CT/150	FAA	LC	1997
FedEx	Memphis, TN	DC-10-10	CF6-6	CAE	FFS	SP1/4w	FAA	LC	1983
FedEx	Memphis, TN	DC-10-10	CF6-6	L-3 Link UK	FFS	SP1/4w	FAA	LC	1983
FedEx	Memphis, TN	MD-10-10		CAE	FFS	EP1000CT/150	FAA	LC	2000

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
FedEx	Memphis, TN	MD-10-10		CAE	FFS	Maxvue+/150	FAA	L7	2000
FedEx	Memphis, TN	MD-11F	CF6-80C2	CAE	FFS	EP1000CT/150	FAA	LD	1990
FedEx	Memphis, TN	MD-11F	CF6-80C2	CAE	FFS	Maxvue+/150	FAA	L6	1998
FedEx	Memphis, TN	MD-11F	CF6-80C2	CAE	FFS	EP1000CT/150	FAA	LD	
FedEx	Memphis, TN	MD-11F	CF6-80C2	CAE	FFS	Maxvue+/150	FAA	L6	1998
FedEx	Memphis, TN	MD-11F	CF6-80C2	CAE	FFS	EP1000CT/150	FAA	LD	1998
FlightSafety International (Atlanta)	Atlanta, GA	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII+/180	FAA, MDGAC	LD	2000
FlightSafety International (Atlanta)	Atlanta, GA	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII+/180	FAA, MDGAC	LD	2000
FlightSafety International (Atlanta)	Atlanta, GA	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII+/180	FAA, MDGAC	LD	2001
FlightSafety International (Atlanta)	Atlanta, GA	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/180	FAA, MDGAC	LD	2001
FlightSafety International (Atlanta)	Atlanta, GA	CRJ700	CF34-8C1	FSI	FFS	Vital IX/180	FAA, MDGAC	LD	2003
FlightSafety International (Atlanta)	Atlanta, GA	Dash 8-100/200/300	PW120	FSI	FFS	Vital VIII/180	FAA, UKCAA, TC, MDGAC	LC	2001
FlightSafety International (Atlanta)	Atlanta, GA	EMB-120 Brasilia	PW118	FSI	FFS	Vital IV/4w	FAA, TC, MDGAC	LC	1991
FlightSafety International	Cincinnati,	CRJ100/200	CF34-3A1	FSI	FFS		FAA,	LD	2000

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
(Cincinnati)	KY	/700/900/1000					MDGAC		
FlightSafety International (Cincinnati)	Cincinnati, KY	CRJ100/200/ 700/900/1000	CF34-3A1	FSI	FFS		FAA, MDGAC	LD	2001
FlightSafety International (Cincinnati)	Cincinnati, KY	CRJ100/200/ 700/900/1000	CF34-3A1	FSI	FFS		FAA, MDGAC	LD	2002
FlightSafety International (Cincinnati)	Cincinnati, KY	E-170	CF34-8E5	FSI	FFS		FAA	LD	2013
FlightSafety International (Fort Worth)	Dallas, TX	CRJ200/700	CF34-8C1	FSI	FFS	Vital IX/180	FAA, MDGAC	LD	2003
FlightSafety International (Fort Worth)	Dallas, TX	ERJ-145	AE3007A	FSI	FFS	Vital IX/180	FAA, MDGAC	LD	2004
FlightSafety International (Houston)	Houston, TX	ATR 42	PW120	FSI	FFS	Vital IV/4w	FAA, TC, MDGAC, ANAC	LC	1988
FlightSafety International (Houston)	Houston, TX	ATR 42/72	PW120	FSI	FFS	Vital X/4w	FAA, TC, MDGAC	LC	1991
FlightSafety International (Houston)	Houston, TX	ATR 42/ 72-500	PW127E	FSI	FFS	Vital IX/180	FAA, FTSA, TC, MDGAC, A	LD	2003
FlightSafety International (Houston)	Houston, TX	ERJ-145	AE3007A	FSI	FFS	Vital VIII/180	FAA, FTSA, MDGAC	LD	1998
FlightSafety International	Houston, TX	ERJ-145	AE3007A	FSI	FFS	Vital VIII/150	FAA,	LD	2001

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
(Houston)							MDGAC, UKCAA		
FlightSafety International (Houston)	Houston, TX	ERJ-145	AE3007A	FSI	FFS	Vital IX/180	FAA, FTSA, ANAC-Brazil	LD	2002
FlightSafety International (La Guardia)	La Guardia, NY	Beech 1900D	PT6A-67D	FSI	FFS	Vital VII/180	FAA, TC, MDGAC	LD	1996
FlightSafety International (La Guardia)	La Guardia, NY	Shorts 360	PT6A-65AR	FSI	FFS	Vital IV/4w	FAA, TC, MDGAC	LC	1983
FlightSafety International (Long Beach)	Long Beach, CA	EMB-120 Brasilia	PW118	FSI	FFS	Vital IV/4w	FAA, TC, MDGAC	LC	1990
FlightSafety International (Memphis)	Memphis, TN	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/150	FAA, MDGAC	LD	2001
FlightSafety International (Memphis)	Memphis, TN	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/150	FAA, MDGAC	LD	2000
FlightSafety International (Memphis)	Memphis, TN	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/150	FAA, MDGAC	LD	1997
FlightSafety International (Salt Lake)	Salt Lake, UT	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/180	FAA, MDGAC	LD	2001
FlightSafety International (Salt Lake)	Salt Lake, UT	CRJ100/200	CF34-3A1	FSI	FFS	Vital VIII/180	FAA, MDGAC	LD	1999
FlightSafety International (Salt Lake)	Salt Lake, UT	CRJ200/700	CF34-3A1	FSI	FFS	Vital VIII/180	FAA, MDGAC	LD	2002

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
FlightSafety International (Salt Lake)	Salt Lake, UT	CRJ700	CF34-8C5B1	FSI	FFS	Vital X/160	FAA, MDGAC	LD	2011
FlightSafety International (San Antonio)	San Antonio, TX	Metro C-26	TPE331-12UAR-701G	FSI	FTD	Vital VIII+/4w	FAA, TC, MDGAC	LC	1995
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Beech 1900D	PT6A-67D	FSI	FFS	Vital VII/4w	FAA, TC, MDGAC	LD	1996
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Dash 8 Q100/200/300	PW120A	FSI	FFS		JCAB	LC	2011
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Dash 8 Q400	PW150A	FSI	FFS	Vital X/180	FAA, TC, MDGAC	LD	2000
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Dash 8 Q400	PW150A	FSI	FFS	Vital IX/180	FAA, TC, MDGAC	LD	2007
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Dash 8-100/200/300	PW120	FSI	FFS	Vital VIII/4w	FAA, TC, MDGAC, UKCAA	LC	1992
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Dash 8-100/300	PW120	FSI	FFS	Vital VII/4w	FAA, TC, MDGAC, UKCAA	LC	1994
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Jetstream 31/32	TPE331-10	FSI	FFS		FAA, TC, MDGAC	LC	1991
FlightSafety International (Seattle Sea-Tac)	Seattle, WA	Metro III	TPE331-11U	FSI	FTD	SP1/2w	FAA, TC, MDGAC	LB	1991
FlightSafety International (St Louis)	St Louis, MO	CRJ200	CF34-3B1	FSI	FFS	Vital IX/180	FAA, TC,	LD	2007

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
							CAAC, MDGAC		
FlightSafety International (St Louis)	St Louis, MO	CRJ700	CF34-8C1	FSI	FFS		FAA, MDGAC, CAAC, TC	LD	2008
FlightSafety International (St Louis)	St Louis, MO	CRJ700/900	CF34-8C1	FSI	FFS	Vital IX/180	FAA, TC, MDGAC, CAAC	LD	2006
FlightSafety International (St Louis)	St Louis, MO	Dash 8 Q400	PW150A	FSI	FFS	Vital IX/180	FAA, TC, MDGAC	LD	2008
FlightSafety International (St Louis)	St Louis, MO	E-170	CF34-8E5	FSI	FFS	Vital IX/180	FAA, MDGAC	LD	2006
FlightSafety International (St Louis)	St Louis, MO	E-170	CF34-8E5	FSI	FFS	Vital IX/180	FAA, MDGAC	LD	2008
FlightSafety International (St Louis)	St Louis, MO	E-170	CF34-8E5	FSI	FFS	Vital IX/180	FAA, ANAC Brazil, MDG	LD	2006
FlightSafety International (St Louis)	St Louis, MO	ERJ-135/145	AE3007A	FSI	FFS	Vital X/180	FAA, UKCAA, ANAC Brazil	LD	2002
FlightSafety International (St Louis)	St Louis, MO	ERJ-135/145	AE3007A	FSI	FFS	Vital VIII/180	FAA, UKCAA,	LD	2000

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
							MDGAC		
FlightSafety International (St Louis)	St Louis, MO	ERJ-135/145	AE3007A	FSI	FFS	Vital IX/180	FAA, UKCAA, MDGAC	LD	2002
FlightSafety International (St Louis)	St Louis, MO	Jetstream 31/32	TPE331-10	FSI	FFS	Vital IV/4w	FAA, TC, MDGAC	LC	1989
FlightSafety International (St Louis)	St Louis, MO	Metro III	TPE331-11U	FSI	FFS		FAA, TC, MDGAC	LB	1986
JetBlue Airways	Orlando, FL	A320		CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	A320		CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	A320		CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	A320		CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	E-170	CF34-8E	CAE	FFS	Tropos/180	FAA	LD	2007
JetBlue Airways	Orlando, FL	E-190	CF34-10E	CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	E-190	CF34-10E	CAE	FFS	Tropos/180	FAA	LD	2005
JetBlue Airways	Orlando, FL	E-190	CF34-10E	CAE	FFS	Tropos/180	FAA	LD	2006
National Aeronautical Space Administration (NASA) Ames Research Center	Moffett Field, CA	747-400	PW4000	CAE	FFS	Vital VIII/180	FAA	LD	1993
PanAm International Flight Academy (Cincinnati)	Cincinnati, KY	727-200	JT8D-15	Link	FFS	Vital IV/4w	FAA	LC	1979

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
PanAm International Flight Academy (Cincinnati)	Cincinnati, KY	A300B4	CF6-50C2	L-3 Link UK	FFS	Vital IV/4w	FAA	LC	1980
PanAm International Flight Academy (Cincinnati)	Cincinnati, KY	DC-8-71	CFM56-2	Link	FTD	SP1/2w	FAA	LB	1994
PanAm International Flight Academy (Denver)	Denver, CO	737-300	CFM56-3B	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	747-400	PW 4056	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	747-400	PW 4056, CF6-80, RB211-524	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	757	PW2037	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	757	RB211-535	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	767	PW 4052/4060	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	767	PW 4060	CAE	FFS		FAA	LC	
PanAm International Flight Academy (Denver)	Denver, CO	767	PW JT9D-7R-4D	CAE	FFS		FAA	LC	
PanAm International Flight Academy (Denver)	Denver, CO	777	PW 4077, PW4090, GE90	Thomson	FFS		FAA	LD	

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
PanAm International Flight Academy (Denver)	Denver, CO	A320	V2527-A5	L-3 Link UK	FFS		FAA	LD	
PanAm International Flight Academy (Denver)	Denver, CO	A320	V2527-A5	Thomson	FFS		FAA	LD	
PanAm International Flight Academy (Las Vegas)	Las Vegas, NV	737-200	JT8D-9	CAE	FFS	SP1T	FAA	LC	1986
PanAm International Flight Academy (Las Vegas)	Las Vegas, NV	737-800W	CFM56-7B	Sim-Industries	FFS	EP1000CT	FAA	LD	
PanAm International Flight Academy (Las Vegas)	Las Vegas, NV	MD-82/83	JT8D-217	L-3 Link UK	FFS	SP-X 250	FAA	LC	1989
PanAm International Flight Academy (Las Vegas)	Las Vegas, NV	MD-88	JT8D-217C/219	CAE	FFS	Vital IV/4w	FAA	LC	
PanAm International Flight Academy (Memphis)	Memphis, TN	727-200	JT8D-15	CAE	FFS	SP3-T	FAA	LC	1984
PanAm International Flight Academy (Memphis)	Memphis, TN	DC-10-30	CF6-50C	CAE	FFS	ESIG3350T	FAA	LC	1981
PanAm International Flight Academy (Memphis)	Memphis, TN	MD-11	PW 4462	CAE	FFS		FAA	LD	

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
PanAm International Flight Academy (Miami)	Miami, FL	707	JT3D-3	Link	FTD	SP1	FAA	LA	1966
PanAm International Flight Academy (Miami)	Miami, FL	727-200	JT8D-15	CAE	FFS	SP1/4w	FAA	LC	1981
PanAm International Flight Academy (Miami)	Miami, FL	737-200	JT8D-15	CAE	FFS	Raster NX1/4w	FAA	LC	1982
PanAm International Flight Academy (Miami)	Miami, FL	737-200	JT8D-15A	L-3 Link UK	FFS	SP1	FA	LC	1975
PanAm International Flight Academy (Miami)	Miami, FL	737-300	CFM56-3B1	CAE	FFS	Raster NX1/4w	FAA	LC	1994
PanAm International Flight Academy (Miami)	Miami, FL	737-400	CFM56-3B1	L-3 Link UK	FFS	Raster Flite	FAA	LC	2006
PanAm International Flight Academy (Miami)	Miami, FL	737-800W	CFM56-7B	Rockwell Collins	FFS	EP1000CT	FAA	LC	2010
PanAm International Flight Academy (Miami)	Miami, FL	737-800W	CFM56-7B	Sim-Industries	FFS	EP1000CT	FAA	LC	2009
PanAm International Flight Academy (Miami)	Miami, FL	737-800W	CFM56-7B	Sim-Industries	FFS	EP1000CT	FAA	LD	2011
PanAm International Flight Academy (Miami)	Miami, FL	747-200F	CF6-50E2	Link-AST	FFS	Raster XT	FAA	LC	1982
PanAm International Flight Academy (Miami)	Miami, FL	747-200F	CF6-50E2	Link-AST	FFS	SP1-T	FAA	LC	1990
PanAm International Flight Academy (Miami)	Miami, FL	747-300	CF6-50E2	L-3 Link UK	FFS		FAA	LC	1983

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
PanAm International Flight Academy (Miami)	Miami, FL	747-400F	CF6-80C2B5F	CAE	FFS	Tropos 6000	FAA	LD	1996
PanAm International Flight Academy (Miami)	Miami, FL	747-400F	CF6-80C2B5F	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Miami)	Miami, FL	757	PW2037/ RB211-535	FSI	FFS		FAA	LC	
PanAm International Flight Academy (Miami)	Miami, FL	757	PW2037/ RB211-535	L-3 Link UK	FFS		FAA	LD	
PanAm International Flight Academy (Miami)	Miami, FL	767	CF6-80A, JT9D-7R4D	L-3 Link UK	FFS	Raster Flight	FAA	LC	
PanAm International Flight Academy (Miami)	Miami, FL	767	JT9D-7	CAE	FFS	SP-X 500	FAA	LC	1990
PanAm International Flight Academy (Miami)	Miami, FL	767	JT9D-7/CF6-80A	L-3 Link UK	FFS	SP-X 250	FAA	LC	1983
PanAm International Flight Academy (Miami)	Miami, FL	777	GE90-115/-94B	FSI	FFS		FAA	LD	1996
PanAm International Flight Academy (Miami)	Miami, FL	777-200	PW4000	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Miami)	Miami, FL	A320-200	CFM56-5B4/IAE V2527-A5	CAE	FFS		FAA	LD	
PanAm International Flight Academy (Miami)	Miami, FL	A320-200	V2500	CAE	FFS		FAA	LC	1989
PanAm International	Miami, FL	DC-10-10/30	CF6	CAE	FFS	SP1	FAA	LC	1983

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
Flight Academy (Miami)									
PanAm International Flight Academy (Miami)	Miami, FL	DC-8-71	CFM56	Conductron	FFS		FAA	LC	
PanAm International Flight Academy (Miami)	Miami, FL	DC-9-30	JT8D-9A	Link	FFS	Vital IV/4w	FAA	LC	1969
PanAm International Flight Academy (Miami)	Miami, FL	MD-80	JT8D-217/219	CAE	FFS	Raster Flite/4w	FAA	LC	1983
PanAm International Flight Academy (Miami)	Miami, FL	MD-82	JT8D-217	L-3 Link UK	FFS	SP-X 200	FAA	LC	1993
PanAm International Flight Academy (Miami)	Miami, FL	MD-88	JT8D-217/219	L-3 Link UK	FFS	Raster Flite	FAA	LC	1988
PanAm International Flight Academy (Minneapolis)	Minneapolis, MN	CRJ200	CF34-3A1	CAE	FFS	Maxvue+/180	FAA	LD	2000
PanAm International Flight Academy (Minneapolis)	Minneapolis, MN	CRJ700/900	CF34-8C5	FSI	FFS	Vital IV	FAA	LD	2008
PanAm International Flight Academy (Minneapolis)	Minneapolis, MN	E-175/195	CF34-8	FSI	FFS	Vital X	FAA	LD	2009
Purdue University	West LaFayette, IN	727-100	JT8D	CAE	FTD	N6000/2w	FAA	LA	1994
Purdue University	West LaFayette, IN	727-200	JT8D	CAE	FFS	Image III/4w	FAA	LC	1982

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
SimCom (Orlando)	Orlando, FL	Dornier 328Jet	PW306B	CAE	FFS	Maxvue+/180	FAA	LD	2001
SimCom (Orlando)	Orlando, FL	Jetstream 41	TPE331-146GR/HR	CAE	FFS	SPX500HT/W	FAA	LC	1995
Southwest Airlines	Dallas, TX	737-200	JT8D	L-3 Link UK	FFS	SP1/2w	FAA	L6	1966
Southwest Airlines	Dallas, TX	737-300	CFM56-3	CAE	FFS	ESIG3350/150	FAA	LC	1994
Southwest Airlines	Dallas, TX	737-300	CFM56-3	L-3 Link UK	FFS	ESIG3350/150	FAA	LC	1986
Southwest Airlines	Dallas, TX	737-300	CFM56-3	L-3 Link UK	FFS	ESIG3350/150	FAA	LC	1984
Southwest Airlines	Dallas, TX	737-700	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LC	2002
Southwest Airlines	Dallas, TX	737-700	CFM56-7	CAE	FFS	ESIG3350/180	FAA	LC	2006
Southwest Airlines	Dallas, TX	737-700	CFM56-7	CAE	FFS			LD	2002
Southwest Airlines	Dallas, TX	737-700	CFM56-7	L-3 Link UK	FFS	ESIG3350/180	FAA	LC	1997
Southwest Airlines	Dallas, TX	737NG		CAE	FFS	Tropos 6000	FAA	LD	2009
Spiral Aviation Training (SATCO)	Englewood, CO	Beech 1900D		SATCO	FFS	Raster NX1/4w	FAA	LC	2002
United Airlines (Denver)	Denver, CO	737-200	JT8D-17	CAE	FFS	SPX550/4w	FAA	LD	1987
United Airlines (Denver)	Denver, CO	737-300	CFM56-3B1	CAE	FFS	SP1T	FAA	LD	1989

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
United Airlines (Denver)	Denver, CO	737-300	CFM56-3B2	CAE	FFS	SP1T	FAA	LD	1987
United Airlines (Denver)	Denver, CO	737-300	CFM56-3B2	CAE	FFS	SP1T	FAA	LC	1988
United Airlines (Denver)	Denver, CO	747-200	CF6	CAE	FFS		FAA	LC	2006
United Airlines (Denver)	Denver, CO	747-200	JT9D-7A	CAE	FFS		FAA	LC	1992
United Airlines (Denver)	Denver, CO	747-400	PW4056	CAE	FFS	SPX500HT/150	FAA	LD	1989
United Airlines (Denver)	Denver, CO	747-400	PW4056	CAE	FFS	SPX500HT/150	FAA	LD	1993
United Airlines (Denver)	Denver, CO	747-400	PW4056, CF6, RB211	CAE	FFS	ESIG3350/150	FAA	LD	1998
United Airlines (Denver)	Denver, CO	747-400	PW4056, CF6, RB211	CAE	FFS	ESIG3350/150	FAA	LD	1998
United Airlines (Denver)	Denver, CO	757-200	PW2037	CAE	FFS	SPX250/4w	FAA	LD	1992
United Airlines (Denver)	Denver, CO	757-200	PW2037	CAE	FFS	SPX250/4w	FAA	LD	1991
United Airlines (Denver)	Denver, CO	757-200ER	PW2037, RB211	CAE	FFS	ESIG3350/150	FAA	LD	1997
United Airlines (Denver)	Denver, CO	767-200	JT9D	CAE	FFS	SP1T/4w	FAA	LC	1989
United Airlines (Denver)	Denver, CO	767-300ER	PW4052/4060	CAE	FFS	ESIG3350/180	FAA	LD	2000
United Airlines (Denver)	Denver, CO	767-300ER	PW4060	CAE	FFS	SP1T/4w	FAA	LC	1992

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
United Airlines (Denver)	Denver, CO	777-200	GE, P&W, RR	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1997
United Airlines (Denver)	Denver, CO	777-200	GE, P&W, RR	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1994
United Airlines (Denver)	Denver, CO	777-200	GE, P&W, RR	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1997
United Airlines (Denver)	Denver, CO	A320-200	V2527-A5	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	2002
United Airlines (Denver)	Denver, CO	A320-200	V2527-A5	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1994
United Airlines (Denver)	Denver, CO	A320-200	V2527-A5	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1997
United Airlines (Denver)	Denver, CO	A320-200	V2527-A5, CFM56	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1998
United Airlines (Denver)	Denver, CO	A320-200	V2527-A5, CFM56	L-3 Link UK	FFS	ESIG3350/150	FAA	LD	1999
United Airlines (Houston)	Houston, TX	737-300	CFM56-3	Conductron	FFS	Vital IV/4w	FAA	LC	1982
United Airlines (Houston)	Houston, TX	737-500	CFM56-3	L-3 Link UK	FFS	Maxvue+/180	FAA	LC	1994
United Airlines (Houston)	Houston, TX	737-700/800	CFM56-7	CAE	FFS	Maxvue+/180	FAA	LC	1999
United Airlines (Houston)	Houston, TX	737-800		CAE	FFS	Tropos	FAA	LD	2009
United Airlines (Houston)	Houston, TX	737-800	CFM56-7	CAE	FFS	Tropos	FAA	LD	2007

Operator USA	Location and	A/C type	Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
United Airlines (Houston)	Houston, TX	757-200	PW2037	L-3 Link UK	FFS	Maxvue+/150	FAA	LC	1995
United Airlines (Houston)	Houston, TX	767-400ER	CF6-80C2	CAE	FFS	Maxvue+/180	FAA	LD	1999
United Airlines (Houston)	Houston, TX	777-200	GE90-92B	CAE	FFS	Maxvue+/180	FAA	L6	1999
United Airlines (Houston)	Houston, TX	787		CAE	FFS	Tropos 6000LCos	FAA	LD	2008
UPS Airlines	Louisville, KY	727-100QF	Tay	L-3 Link UK	FFS	SPX250/150	FAA	LD	1991
UPS Airlines	Louisville, KY	747-400F/8F		CAE	FFS	EP1000CT	FAA	LD	2008
UPS Airlines	Louisville, KY	757-200PF	PW2040	L-3 Link UK	FFS	SPX500HT/150	FAA	LD	1990
UPS Airlines	Louisville, KY	757-200PF	RB211	L-3 Link UK	FFS	SPX250/150	FAA	LD	1995
UPS Airlines	Louisville, KY	767-300ER		L-3 Link UK	FFS	EP1000CT	FAA	LD	2009
UPS Airlines	Louisville, KY	A300-600F	PW4158	L-3 Link UK	FFS	ESIG3800/180	FAA	LD	2000
UPS Airlines	Louisville, KY	DC-8-71	CFM56-2	L-3 Link UK	FFS	SPX250/150	FAA	LD	1991
UPS Airlines	Louisville, KY	MD-11F	GE, P&W	CAE	FFS	SPX500HT/150	FAA	LD	1990

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
US Airways Training Center (Charlotte)	Charlotte, NC	CRJ200	CF34-3A1	CAE	FFS	Maxvue+/180	FAA	LD	2000
US Airways Training Center (Charlotte)	Charlotte, NC	CRJ200/700	CF34-3A1/3B1/8C1	CAE	FFS	Maxvue+/180	FAA	LD	2002
US Airways Training Center (Phoenix)	Phoenix, AZ	737-200	JT8D-15	CAE	FTD	SP1/4w	FAA	LB	1986
US Airways Training Center (Phoenix)	Phoenix, AZ	737-300	CFM56-3	CAE	FFS	Image IIT/4w	FAA	LC	1988
US Airways Training Center (Phoenix)	Phoenix, AZ	737-300	CFM56-3	CAE	FFS	Image IIT/4w	FAA	LC	1988
US Airways Training Center (Phoenix)	Phoenix, AZ	737-300	CFM56-3	CAE	FFS	Vital VII/4w	FAA	LD	1988
US Airways Training Center (Phoenix)	Phoenix, AZ	737-300/400	CFM56-3	CAE	FFS	SPX200/4w	FAA	LC	1992
US Airways Training Center (Phoenix)	Phoenix, AZ	757-200	PW2037	CAE	FFS	Vital IV/4w	FAA	LC	1982
US Airways Training Center (Phoenix)	Phoenix, AZ	757-200ER	RB211	CAE	FFS	SPX200/4w	FAA	LC	1990
US Airways Training Center (Phoenix)	Phoenix, AZ	A320		CAE	FFS	Tropos 6000	FAA	LD	2008
US Airways Training Center (Phoenix)	Phoenix, AZ	A320		CAE	FFS	Tropos 6000	FAA	LD	2008
US Airways Training Center (Phoenix)	Phoenix, AZ	A320		CAE	FFS 7000	Tropos 6000		LD	2012

Operator USA	Location and A/C type		Engines	Simulator OEM	Sim. type	Visual Display	Authority	CertIF	Entry
US Airways Training Center (Phoenix)	Phoenix, AZ	A320-200		L-3 Link UK					2002
US Airways Training Center (Phoenix)	Phoenix, AZ	A320-200	V2500	CAE	FFS	Maxvue+/180	FAA	LD	1999
US Airways Training Center (Phoenix)	Phoenix, AZ	A320-200	V2500	CAE	FFS	Maxvue+/180	FAA	LD	1999
US Airways Training Center (Phoenix)	Phoenix, AZ	A320-200	V2500-A1	CAE	FFS	SPX200/4w	FAA	LC	1992
US Airways Training Center (Phoenix)	Phoenix, AZ	A320-200	V2500-A1	L-3 Link UK	FFS	SP1T/4w	FAA	LC	1991
US Airways Training Center (Phoenix)	Phoenix, AZ	A330/A340		CAE	FFS	Tropos 6000		LD	2008
US Airways Training Center (Phoenix)	Phoenix, AZ	A330-300	PW4168A	CAE	FFS	Maxvue+/180	FAA	LD	1999
US Airways Training Center (Phoenix)	Phoenix, AZ	Dash 8-100A	PW123	CAE	FFS	Image IIT/4w	FAA	LC	1992
US Airways Training Center (Phoenix)	Phoenix, AZ	E-170		CAE	FFS	Maxvue	FAA	LD	2004

2.2.2 ENGINEERING SIMULATORS

Engineering and research simulators have certain key functions present, in order for it to be a viable engineering development, research, and test system. Key, functional base capabilities include:

- Base virtualization system (Linux/Berkeley Software Distribution (BSD)/Greenfield)
- Cockpit visualization
- Model visualization
- Customizable boot-strap loader
- Virtual Systems Management
- Inter-VM or Inter-Simulation Module data communications virtualization
- Simulation configuration management to load new aircraft models or new/modified aircraft systems
- Remote/other simulation systems, component module communications, and hardware-in-the-loop adapters
- External communications input and output simulation
- Power-up and ready to initiate (i.e., module boot-up sequence, simulation start, etc.)

In examining engineering simulators, the FAA has four options for their cyber security simulators:

1. Custom-designed and coded
2. COTS Simulators
3. Open source simulators
4. A combination of COTS and open source modules

All options can be made to utilize or link to, existing full or partial (i.e., engines) simulations whether commercial, government, or academic via a software communications adapter module.

The first option is prohibitively expensive, and requires the FAA to have long-term staff to maintain, update, and add new functionality (i.e., AAtS, NextGen). Although possibly the most flexible option due to the development costs and long-term staffing requirements to support it, we do not recommended Option 1 for FAA's consideration.

The second option is to utilize COTS simulation products as the base simulator. Leading, COTS simulation providers offer the capabilities to mix new or updated user coded modules into their systems. They also validate their aircraft simulator models with the airframer to ensure that they have a true aircraft model on which their customers can develop. The key criteria here are the long-term viability of the provider; purchasing, maintenance, and custom support costs; and, the basic features to support development and research (i.e., software re-configurable).

The third option is to utilize one of the Open Source Simulators; there are both, truly open public and government-developed bases. These are essentially free, but come with some open source stipulations requiring evaluation. Again, the key issue is the long-term viability of the open source base (i.e., trust that it will forever move forward with more capabilities and aircraft model support).

The fourth option is to utilize a combination of both COTS products, and open source modules. In this case, a selection between COTS and open source simulation foundation would need to be made, and then the addition of either COTS or open source modules for specific simulation requirements (i.e., cyber security testing, new flight controls concepts).

COTS Flight Simulators

As FAA-approved Personal Computer-based Aviation Training Devices (PCATDs) gain wider acceptance each year, the distinctions between simulation games and simulation devices blurred, and the aviation training industry began taking more interest in the realism companies were offering in their add-ons to flight simulators.

Today, COTS flight simulators are minimal in cost, and available for download from the Internet. Table 3 identifies sites providing valuable solutions and utilizing simulation to perform analysis on safety only.

TABLE 3. COTS FLIGHT SIMULATOR PRODUCTS

COTS Product	Web Site
Simulator Communication Systems (SCS) has created simulators for both professional and hobbyist, alike. The SCS product line allows the creation of simulator-independent software, and provides a solution for connecting replica and real avionic components to specific simulators.	Cross-Simulator.com
ELITE Simulation Solutions is a global provider of Instrument Flight Rules (IFR) training software, flight controls, and flight training devices. They specialize in building and supporting FAA and JAR-certified trainers, and offer custom programming to both private and government entities.	FlyElite.com
Project Magenta has become a very recognizable name in Flight Simulation and Pilot Training with several thousand installations to date, from desktop systems to certified or approved Flight Training Devices. The product range spans from type-specific glass cockpits, flight management systems, and interfacing software, to data logging and traditional IFR training software. Project Magenta software can be used in conjunction with Flight Simulators as well as Stand-Alone Solutions – Data Playback is also possible.	ProjectMagenta.com
Commercial Level Simulations (CLS) is a unique company for Flight Simulation. Founded in 2005 by Warren C. Daniel and Albert Bouwman, CLS has grown quickly to its current position of virtual simulator products. CLS creates many products for a variety of customers to enjoy, as well as business and military solutions.	CommercialLevel.com
Integrated Simavionics provides a set of gauges integrated with FMS units as an avionics panel upgrade for Microsoft	isgism.com

COTS Product	Web Site
Flight Simulator 2004 and Flight Simulator X aircraft.	
Boeing provides a wide range of simulator software updates and hardware upgrades used to provide better fidelity and flexibility of training devices. Boeing has the experience and capability to conduct updates across a wide range of device types, makes, and models. Services include implementation of new aerodynamics, engine and flight controls, model upgrades, visual system, EFB upgrades, and configuration changes.	Boeing.com
GEFS is a free, online, flight simulator based on Google Earth.	Gefs-online.com
FlightSim provides a large set of products for simulators.	Flightsim.com
Flyanarliner provides training and products for simulation.	Flyanairliner.com
iAircraft is an aircraft simulation modeling package designed specifically for use in aircraft test lab facilities such as "iron bird" simulators and simulation-based avionics integration test facilities. iAircraft's development was for the simulation of commercial aircraft, and can be parameterized to represent a wide range of fixed-wing aircraft. iAircraft is composed of up of a collection of Simulink models that may be run within the Simulink simulation software, or on Advantage based real-time simulation computer systems (rtX, rtX-V, etc.). iAircraft development includes an architecture that allows the aircraft simulation to get up and running quickly in pure simulation mode, but also makes it easy to connect to a real aircraft LRU for performing aircraft hardware-in-the-loop testing, integration, and avionics verification activities. The iAircraft simulation modeling methodology is based on commercial aircraft industry-leading R&D for several decades.	adi.com
SimCheck International was established in 1990, and is recognized as a global leader in providing flight-training organizations with affordable, high fidelity, flight simulation components, and systems. SimCheck Int.'s PFC's systems simulate dozens of general aviation and commercial aircraft, as well as today's most popular technically advanced aircraft.	SimCheck International
Shareware sites	2000 Shareware.com Winsite.com

2.3 GOVERNMENT LABORATORIES

2.3.1 FAA CIS LABORATORIES

The Florida NextGen Test Bed (Test Bed) is an FAA initiative to develop a NextGen research and demonstration facility at the Daytona Beach International Airport (DAB) in Florida. Development of the Test Bed provides NextGen stakeholders with rapid integration capability for testing NextGen Operational Improvements (OI) and Enablers by leveraging NAS systems with prototype capabilities. It utilizes a cost-effective and scalable architecture to allow for growth as OIs and enablers evolve. The Test Bed will integrate and demonstrate new and emerging technologies into existing and planned enhancements for the NAS.

Governed by the FAA and used by NextGen stakeholders within industry, academia, and government, the Test Bed's intent is to provide a forum to help foster NextGen partnerships within industry, academia, and government by providing a facility for integration and the demonstration of new capabilities. Its administration is through the FAA Tech Center in Atlantic City. Harris Corporation and Emery-Riddle University jointly operates the Florida facility.

TABLE 4. FAA CONCEPT AND INTEGRATION (CSI) LABORATORIES

FAA CSI Web Sites
En Route Integration and Interoperability Facility (EIIF)
Oceanic Integration and Interoperability Facility (OIIF)
NextGen Integration and Evaluation Capability (NIEC)
Research Development & Human Factors Laboratory (RDHFL)
Florida NextGen Test Bed (FTB)

2.3.2 AVIATION COMMUNICATION TESTING LABORATORY

MTI Systems develops, maintains, works with tools supporting several NASA projects and determines appropriate means of verifying the results and supporting any necessary certification, accreditation, or other fit-for-use demonstrations. Relevant work includes:

- Integrated availability analysis for NASA's Communications, Navigation, and Networking, Reconfigurable Testbed (CoNNeCT) onboard the International Space Station (ISS), including link budget models, thermal models, orbit propagation, ISS spacewalk and docking/undocking event projections, and other factors

- Communication system and protocol modeling for new data links and stacks to integrate Unmanned Aerial Vehicles UAVs into the National Airspace System (NAS) for NASA's Unmanned Aircraft Systems (UAS) project

- Analysis of network loading models, virtual machine resource models, and other system performance models used for sizing blade servers and other systems in NASA's Space Network Ground Segment Sustainment (SGSS) project

TABLE 5. AVIATION COMMUNICATION TESTING LABORATORY

Aviation Communication Testing Laboratory Web Site
Aviation Communication Testing Laboratory Operated by MTI SYSTEMS 7833 Walker Drive, Suite 660 Greenbelt, MD, 20770 Contact: Colleen McGraw Colleen@mti-systems.com 410-507-0234

2.3.3 NAVY

The Naval Air Warfare Center, Aircraft Division (NAWCAD) is the full spectrum research, development, test, and evaluation (RDT&E), engineering and fleet support center for air platforms. NAWCAD performs testing in areas such as aircraft systems (manned and unmanned), airborne technology, propulsion, flight test and engineering, avionics design and production, human systems, and aircraft-platform interface.

TABLE 6. NAWCAD

NAWCAD Web Site
Office of Naval Research Summer Faculty Research and Sabbatical Leave Program

2.3.4 NASA

NASA's Aviation Systems Division houses some of the most sophisticated simulation facilities in the world. They support a wide range of research with emphasis on aerospace vehicles, aerospace systems and operations, human factors, accident investigations, and studies aimed at improving aviation safety. The Aviation System's Division collaborates with numerous NASA programs, as well as with other government agencies, industry, and academia, and is strategically important in meeting the Nation's present and future aerospace needs.

The Crew-Vehicle Systems Research Facility (CVSRF) is an unparalleled national resource that supports NASA, the FAA, and many industry research programs. Designed to provide researchers with an environment where they can study how and why aviation errors occur, CVSRF excels in the area of human factors research. NASA's goal is to offer researchers a suite

of simulation facilities and utilities for its use in analyzing flight crew performance, and to develop and improve new simulation and training tools.

CVSRF houses several simulators capable of full-mission simulation. These simulators interact with each other (as well as with other SimLabs facilities) by means of a High Level Architecture (HLA), allowing for enormous flexibility and customization. Using CVSRF's highly sophisticated simulators (the Boeing 747-400, the Advanced Concepts Flight Simulator, and the Air Traffic Control (ATC) Laboratory), researchers are able to study the effects of automation and advanced instrumentation on human performance.

TABLE 7. NASA

NASA Web Site
NASA

2.3.5 UNITED STATES AIR FORCE (USAF)

Wright Patterson Air Force Base (WPAFB) is the home of aeronautical R&D in the USAF. The Aeronautical Systems Center (ASC) develops aircraft for the USAF as part of the Air Force Material Command (AFMC); both organizations' are headquartered here. WPAFB is the home of the Air Force Research Labs (AFRL) headquarters, responsible for the science and technology for the warfighters.

TABLE 8. WPAFB

WPAFB Web Site
Wright Patterson Air Force Base, Ohio

2.4 UNIVERSITY LABORATORIES

2.4.1 VIRGINIA POLYTECH INSTITUTE AND STATE UNIVERSITY

The Vehicle Research and Simulation Laboratory at Virginia Tech houses an i-GATE flight simulator certified by the FAA for instrument flight training. It is capable of simulating up to nine different general aviation aircraft, and provides an avenue for evaluating pilot performance across a range of flight conditions, workload levels, and display modalities.

TABLE 9. VIRGINIA POLYTECH INSTITUTE AND STATE UNIVERSITY

Virginia Polytech Institute and State University Web Site
Virginia Tech College of Engineering - Vehicle and

Virginia Polytech Institute and State University Web Site
Aircraft Research Simulation Lab

2.4.2 THE INSTITUTE OF AVIATION AT THE UNIVERSITY OF ILLINOIS

The Institute of Aviation at the University of Illinois offers a particularly suitable environment for flight training research, and has a pilot training program for undergraduates. Areas of study include:

Flight Simulator Technology

At issue here are questions relating to the appropriate level of flight simulator fidelity that will support the maximum transfer of training to critical aviation skills. Particular interest focuses on visual landings.

Modeling Expert and Novice Flight Performance

Interests focus on understanding the differences between skilled and novice pilots in their control strategies, visual scanning behavior, and decision performance. The goal is to determine the possibility of modeling the characteristics of expertise, to train novice pilots more efficiently.

Microcomputer-based Instruction

Efforts in this area include developing microcomputer technology for instruction of the many procedural aspects of flight related to such areas as ATC communications, pre-flight inspection, decision-making, aircraft systems, and weather. Recent efforts have incorporated multimedia (audio, visual, disk) technology in developing instructional packages.

TABLE 10. INSTITUTE OF AVIATION AT THE UNIVERSITY OF ILLINOIS

Institute of Aviation at the University of Illinois Web Site
Institute of Aviation, University of Illinois at Urbana Champaign

2.4.3 UNIVERSITY OF TORONTO INSTITUTE FOR AEROSPACE STUDIES (UTIAS)

The UTIAS Flight Research Simulator is one of few university-owned, motion-based flight simulators in the world. It allows researchers to experiment with validating improvements in simulator fidelity, and can act as a surrogate for new aircraft designs. This allows researchers to measure human control behavior/performance while flying simulations of these new designs in a virtual environment. In addition, the simulator enables the group's ongoing investigation into a basic understanding of human motion perception and control.

Recently completed projects include:

- Development and testing of an extended B747 flight model that realistically predicts the behavior of the aircraft at, and beyond, stall. The model includes reduced lateral and directional stability, reduced effectiveness of controls, and asymmetric roll-off beyond stall.
- Development of a new adaptive, motion drive algorithm for upset prevention and recovery training (UPRT) that can produce realistic motion cues during the extreme motions encountered during upsets. A set of experiments using this new algorithm determined that good roll cueing leads to improved pilot control, but reduced subjective fidelity, due to the increased lateral side force errors. Therefore, a careful trade-off between the two motions is required for UPRT.
- Development of Bayesian models of human motion perception based on a recent human motion perception study found that translational motion perception tends to follow Weber's law, whereby the just-noticeable-difference (JND) relates linearly to the size of the base stimulus.

TABLE 11. UTIAS

University of Toronto Institute for Aerospace Studies Web Site
University of Toronto Institute for Aerospace Studies

2.4.4 WEST VIRGINIA UNIVERSITY (WVU)

WVU's aerospace program has a strong emphasis on simulation. Students train to use simulation tools throughout their entire curriculum. The laboratory is part of the Bernard Judy Laboratory Wing of the Engineering Science Building (ESB) where its primary use is teaching aircraft simulation. It includes 12 aircraft simulation workstations with D-Six software, etc. Furthermore, the university uses a 6 degree of freedom (DOF) full-motion simulator located in the AERO Lab, next to the low speed wind tunnel. The WVU Lab features' include:

- 6 DOF motion platform driven by electrical induction motors
- Laminar Research X-Plane flight simulation software
- LCD Mosaic Wall four-monitor external visual display
- Instructors operating station
- Computer and control cabinet

The motion platform provides adequate 6 DOF translational and rotational motion cues. Motion drive algorithms convert the motion of the aircraft resulting from the dynamic model into the motion of the platform to optimize the pilot's perception within the physical limitations of the ground-based simulator. For example, constant linear accelerations, sustainable only for a limited time, are simulated by tilting the cockpit at an angular rate below the pilot's perception threshold; the use of gravity simulates the inertial force associated with constant linear acceleration.

TABLE 12. WVU

West Virginia University Web Site
West Virginia University Aircraft Simulation Laboratories

2.4.5 UNIVERSITY OF MARYLAND EASTERN SHORE (UMES)

UMES owns and manages an Advanced Aviation Training Device (AATD) used for research in the following domains:

- Logged Flight Experience
- Instrument Experience
- Instrument Proficiency Check
- Instrument Rating: Practical Test
- Instrument Rating: maximum 20 hours
- Private Pilot Certificate: maximum 2.5 hours
- Commercial Certificate: maximum 50 hours
- Airline Transport Pilot Certificate: maximum 25 hours
- Approved For Use as Limited by Part 141 Appendices

The multi-function display (MFD) simulates more than 12 aircraft, including single-engine, multi-engine, and turboprop aircraft. The system incorporates dual seating and controls for both pilot and co-pilot. This flexibility allows exploration into multiple human factors areas including crew coordination and communication, visual signal detection, auditory signal detection, threat detection and response, aeronautical decision-making, risk tolerance, risk avoidance, and cultural impacts on crew interactions.

These studies may influence the fields of wildlife mitigation, runway incursion avoidance, and aviation security. In addition to human factors research applications, the MFD's facilitate create interactive learning for UMES students enrolled in courses such as Aviation Safety, Advanced Aircraft Systems, and Introduction to Human Factors. Possibilities exist for the MFD to replicate and reconstruct accident scenarios, to demonstrate the operation/failure of systems, and to demonstrate crew interaction principles in a hands-on, immersive environment.

Community outreach purposes, in coordination with the FAA Safety programs taking place on the UMES campus, employ the use of the MFDs. Currently the simulator is being equipped with dual touchscreen LCD monitors for exploration of textual versus audible ATC Instructions. Studies will involve pilot/controller communication errors including errors in readback and hearback. Other planned uses include:

- Surface and Terminal Operations Safety Research
- Navigation, Communication, & Data Transfer
- En route Flight Operations
- Workload Distribution/External Flight Hazards (e.g., Birds)/Human Factors

TABLE 13. UMES

University of Maryland Eastern Shore Web Site
University of Maryland Eastern Shore Engineering Program

2.4.6 THE UNIVERSITY OF TENNESSEE SPACE INSTITUTE (UTSI)

UTSI is a graduate education and research institution located in Tullahoma Tennessee, adjacent to the USAF Arnold Engineering Development Center. Established in 1964 as part of the University of Tennessee, UTSI has become an internationally recognized institution for graduate study and research in engineering, physics, mathematics, and aviation systems. UTSI has made remarkable contributions at the local, state, national, and global levels.

The Aviation Systems Program has major research thrusts in Airborne Science, Systems Engineering & Integration/Space, Integrated Vehicle Health Management, Jet Engine Ground Testing and, Hypersonics. Program faculty, staff, and graduate students conduct exciting and significant research in these areas utilizing their fleet of highly instrumented research aircraft, state-of-the-art research flight simulators, ground testing facilities, advanced instrumentation and data acquisition systems, and modern computational techniques. Led by Professor John Muratore, the Aviation Systems Program is performing Systems Engineering & Integration support for NASA, the USAF, and the aerospace industry.

TABLE 14. UTSI

University of Tennessee Space Institute Web Site
University of Tennessee Space Institute

2.4.7 WICHITA STATE UNIVERSITY (WSU)

Wichita State's dedication is to enhance aviation-related research, education, technology transfer, and utilization in mission critical areas, and to respond to the research interest and needs of the aviation industry through synergistic relationships developed between academia, industry, and government.

Criteria for success:

- The ability of the Center to provide national leadership in making contributions of air transportation problems
- The ability to disseminate results through a continuing education program
- The ability to create self-sufficiency so the Center is not reliant upon funding support from the FAA

NAIR became a core member of the FAA Center of Excellence for General Aviation Research (CGAR) in April 2001.

TABLE 15. WSU

Wichita State University Web Site
Wichita State University National Institute for Aviation Research (NAIR)

2.4.8 EMBRY-RIDDLE AERONAUTICAL UNIVERSITY (ERAU)

The University's fleet of Flight Training Devices (FTDs) is FAA-qualified to L6. Yet, unlike other FAA-qualified FTDs, ERAU's single and multiengine devices include 220-degree, panoramic, visual theaters that enhance the sensation of actual flight. ERAU's Regional Jet FTD includes a 180-degree collimated visual system. No other collegiate flight-training program offers a multimillion-dollar, distributed, simulation network composed of 11 state-of-the-art Frasca FTDs. Embry-Riddle's Advanced Flight Simulation Center houses the following Level 6 FTDs:

- Eight Cessna 172S (Skyhawk)
- Two Diamond DA42 L-360
- One Canadair Regional Jet (CRJ-200)

In addition, ERAU's Aviation Building houses ATC and tower simulators, one motion-based disorientation trainer, and six Basic-Aviation Training Devices (B-ATDs).

TABLE 16. ERAU

Embry-Riddle Aeronautical University Web Site
Embry-Riddle Aeronautical University Daytona Beach

2.4.9 UNIVERSITY OF NORTH DAKOTA (UND)

The John D. Odegard School of Aerospace Sciences at the UND is a world-renowned center for aerospace learning for its achievements in collegiate aviation education, atmospheric research, space studies, and computer science applications. The School is setting the pace for the future of flight boasting over 500 faculty and staff members, over 1,500 students from around the world, and a myriad of programs and projects.

The UND has training and research capability with advanced simulators. The lab features 16 FAA-approved, flight-training devices to prepare students to train in the Cessna 172, Piper Seminole, Schweitzer 300, and Bombardier Canadair Regional Jet aircraft.

TABLE 17. UND

University of North Dakota Web Site
University of North Dakota John D. Odegard School of Aerospace Sciences - Flight Operations

2.5 PRIVATE LABORATORIES

There are private simulation labs and systems across the aviation industry. Largely these consist of the airframers and their supplies. However, these are highly proprietary and not usable in a collaborative research and development environment as the FAA envisions.

It is highly likely that these groups would be interested in using inputs from an FAA base-lined communication's simulation capability including deliberate message manipulation, reply, and

denial of services through either message overload or jamming as part of their certification process.

2.6 SIMULATOR INTEGRABILITY WITH FAA REQUIREMENTS

2.6.1 APPROACH TO COLLABORATION

Our investigation results in the identification of both private and public organizations having the infrastructure and technological capabilities to collaborate with the FAA in research. Aviation is continuously evolving with increasing numbers of new technologies implemented in aircraft. This phenomenon has imposed upon the FAA to redefine its approaches to evaluating risks to the aviation industry. With a limited budget assigned to R&D, collaboration is a plausible conduit for the sharing of resources that minimizes cost, and maximizes benefits.

We have identified seven different types of collaboration models that the FAA can establish with both private and public organizations. The best approach for each case depends on the level of collaboration and the desired outcomes.

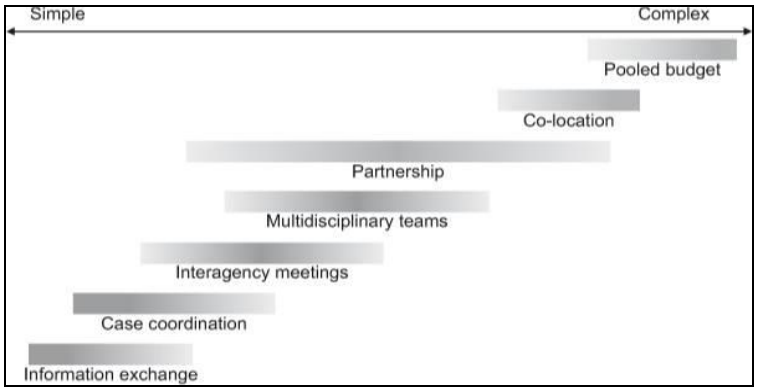
TABLE 18. COLLABORATION MODELS AND DESCRIPTIONS

Collaboration Model	Description
Information exchange	Information exchange between different organizations involved in advance cyber security R&D is the simplest model of collaboration. Its basis is often on informal contacts between professionals in the different organizations who are working with the same set of interests and goals. The exchange of information can be either verbal or in writing, and it can be supported by information and communication technology such as computer platforms or video conferences.
Case coordination	Case coordination is a model where the different organizations involved are not collaborating directly with each other, but indirectly through a person/organization who/that is coordinating their different activities towards an individual project goal.
Interagency meetings	Meetings arranged in connection with specific R&D goals are often interagency meetings. This is a model of collaboration where professionals from the different organizations involved meet to discuss plans and actions that they have in common, sometimes together with the individual concerned. The aim of these meetings is to agree on common activities, sharing resources and results from collaboration.
Multidisciplinary teams	Multidisciplinary teams are used as both a working mode and model of collaboration in specific R&D activities. A group of professionals, from different organizations works together continuously, and over a longer period as a team to reach a predetermined goal or mission, in this model. The different professionals have complementary competences and bring their expertise to the team. There are many different teams with different skillsets. These teams may be multi-professional, inter-professional, and

Collaboration Model	Description
	sometimes even trans-professional, depending on the intensity of the contact among the members and their interdependence.
Partnership	Partnership is a model of collaboration used in many different contexts, and in Aircraft R&D. There are different forms of partnership, but its basis is always in formal agreements between two or more organizations to integrate their services across organizational boundaries. There may be formal agreements on collaboration between the different organizations involved, or formal structures established for communication and exchange of information between these organizations. Such agreements can include different responsibilities and obligations for the organizations involved and can be, more or less formalized, although partnership always means formalization to some extent.
Co-location	Co-location is not so much an organizational model of collaboration, but rather a model of creating favorable conditions for inter-organizational collaboration. In this model, different organizations involved in the same R&D, or parts of these organizations, are located on the same premises. This means a physical proximity, which may have positive effects on the contacts, and the communication between the professionals of the different organizations.
Pooling of budgets	Pooling of budgets is the most complex and demanding model of collaboration. In addition to a close collaboration between the organizations and professionals involved, by pooling financial resources from the different organizations creates a joint budget. The pooled budget is a result of negotiations between the organizations, underpinned with legal arrangements. Its use is to finance joint research activities or projects, planned in collaboration between the organizations involved. Sometimes the organizations also form a separate structure for collaboration, within which different research activities can take place.

Figure 1 illustrates the models of collaboration. The length and darkness of the lines indicates the complexity of the models and their relationship to each other, as well as their variations.

FIGURE 1. MODELS OF COLLABORATION



2.6.2 ISSUES

Due to the complexity of collaboration, collaborative research studies pose significant administrative and professional challenges to organizations seeking common goals. Quite often, stakeholders encounter administrative challenges when they enter into collaborative research studies with individuals outside their organizations, following traditional approaches to projects and data sharing. This includes:

- Competition for limited resources between self-contained research programs, and cross-organizations programs
- Participants in collaborative research studies may have less of a voice in decision- making approaches than are those whose research is exclusive to one organization.

Administrative challenges presented by collaborative research include:

- Promotion and tenure decisions, often organizationally based, making it difficult to assess each individual's contribution to collaborative studies.
- Issues such as authorship, and other forms of "credit". These may be particularly challenging within large collaborations.
- Potential incongruity between an organization's practices encouraging collaborative research and its value on independent work by awarding tenure or promotions.

Researchers in aviation cyber security may face professional issues when engaged in collaborative research, especially when other stakeholders conduct research in separate locations. Examples include:

- Collaborative agreements in which researchers must abide by restrictions placed on the dissemination of findings.
- Distinctly different missions of organizations, government agencies, universities, and industries that may present issues for individual researchers, in university-Government collaborations
- Collaboration among participants in different sectors of the research community, i.e., academic, government, industry, and research institutes may be particularly challenging due to the different operating practices of each sector.

2.6.3 CHALLENGES

Despite the numerous benefits derived from collaboration, challenges can arise at any given time and impact efforts. Finding resources for motivation is one area of critical concern. Likewise, finding a successful organizational structure for the effort, given the diversity of the people and organizations involved, is another area of consideration. It is critical to cement a group vision that does not pull participating organizations away from the original mission. Table 19 presents potential challenges typically faced in a collaboration effort.

TABLE 19. CHALLENGES TO COLLABORATION

Challenge	Challenge Description
Maintenance of group momentum	Frequent staff turnover is the predominant source of this challenge. When this occurs, relationships between organizations must be re-established, slowing the overall forward progress of the group.
Members having difficulties finding enough time	The degree of difficulty noted, regarding finding the time to participate varies considerably from person to person.
Negative reactions of members' constituents	Fears of negative reactions from land trust constituents stemmed from two primary sources: involvement with government partners and a potential association with advocacy organizations working on similar issues. Fears of negative member reactions caused hesitancy among some participants, impeding the progress of the larger group. The challenges created by mixing public and private entities, especially in the field of land conservation, are well known.
Maintaining access to additional funding	Although access to increased funding was cited widely as a benefit to participation, the challenge of maintaining these new levels of support was also frequently discussed.
Increased competition between groups	Currently, geographic differences and thematic differences have made competition between most participating groups minimal to non-existent.
Delayed accomplishments	Although the fundamental purpose of all participating organizations is to protect land, some expressed frustration that their participation in the collaborative effort was not necessarily augmenting this function.
Organizational Structure	
Resources	**Challenge Description**
Difficulty working with a diverse set of organizations	A frequently mentioned challenge centered on working with the diversity of organizations present. Although the networking and learning opportunities provided by other members was

Challenge	Challenge Description
	frequently mentioned as a benefit, many groups struggled with the fact that "we all kind of have different levels of experience.
Duplication of efforts	Overall, very few other large-scale efforts identified as potentially duplicating the work of the collaborative case studies.
Creating an effective structure	Challenges regarding the structure of the group centered on two categories: operating policies, procedures, and issues concerning the group's meetings.
Personalities	When asked to identify the most significant challenge to working with their collaborative effort, one participant remarked, "without a doubt, the biggest challenge is working with those personalities". This was echoed by another participant, who felt that "part of it [the challenge of working together], as always when working with groups, is personalities".
Vision	
Resource	**Challenge Description**
Lack of a shared vision	A major challenge cited was the maintenance of a clear group focus. This is not surprising given the diversity of organizations participating, as discussed above.
Dilemma of mission drift	Potentially even more challenging than defining a vision for the group is adhering to it. According to one Dune Alliance participant, the most significant challenge facing the collaboration is "not changing our mission or our goals to qualify for money".

2.6.4 RISKS

Collaboration presents additional risks associated with the resulting opportunity and benefits; generally, the more formal the relationships, the higher the associated risk. Table 20 identifies some of these risks.

TABLE 20. COLLABORATION RISKS

Risk	Risk Description
Management of Intellectual Property	The collaboration process needs to provide adequate protection of intellectual property.
Data Security/Integrity	Protection of collaborator data and assurance of the integrity of data received.

Risk	Risk Description
Reputational Risk	Effect of ethical violations and the delivery of poor quality and guilt by association.
Stakeholder Privacy	Disclosure of a collaborator's private information.
Increased Awareness	Increased potential for "bad actor" awareness of threat and vulnerabilities.

3. AIRCRAFT CYBER ANALYSIS AND THREAT SIMULATOR (ACATS) PHYSICAL VIRTUALIZATION, AND CYBER TESTING SYSTEM ARCHITECTURE

3.1 PURPOSE

This section documents the foundational architectures required to host an aircraft flight simulation also designed to support cyber security runtime testing of that simulation for cyber vulnerabilities.

Virtualized simulators have a complex physical and virtualization architecture, equally complex to suites of aircraft models and its types of testing. It requires an integrated architectural design incorporating the physical systems on which it operates with virtualization and configuration management; high performance networks both to move data, and to ensure that the simulation models can exchange data within very smalltime increments, down to milliseconds to simulate aircraft performance; and, local storage during the simulation runs and long term bulk storage for the output of runs, data analysis, model components, configurations, etc. Virtualized simulations add to the processing capacity required to run them.

Cyber testing with a simulation model adds complexity to the simulation, the physical, and virtualization architectural foundation required. Injecting cyber tests to the simulation adds processor capacity and storage requirements, as well as the network complexity especially to support.

The ACATS is a collection of systems, networks, devices, and tools for the security analysis of aviation systems to develop cyber security strategies engaged in threat analysis and information sharing, and to provide input to regulatory bodies for protecting this critical infrastructure. Its short- and long-term goals include:

- Penetration testing and analysis of simulated and real aviation systems, such as:
    - Multiple aircraft models,
    - Ground communication and support systems, and
    - External and internal probe points (e.g., PIES/Passenger Owned Devices (PODS))
- Through virtualization, top-down and bottom-up simulation of aviation components including:
    - Aircraft and support components
    - Airports, airlines, and maintenance facilities
    - Stationary, ready, and in-motion aircraft
- Classification and disclosure of aviation cyber threats, and vulnerabilities
- Segmental infrastructure to support partnership with aviation manufacturers, sponsored and academic research, US and International law enforcement, and other governmental entities

The approach taken is one of incremental growth, with a picture of the whole, offered. Figure 2 illustrates a macro view of the ACATS and its three tiers.

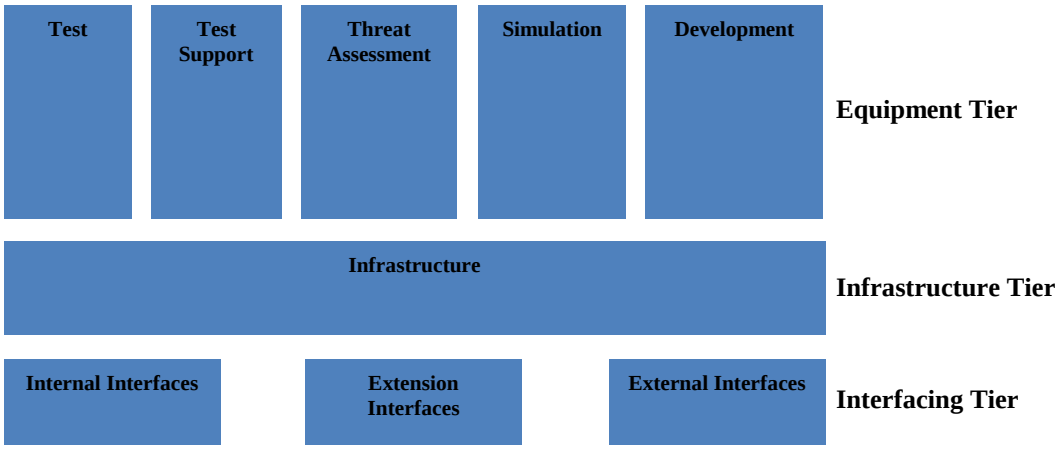


FIGURE 2. ACATS MACRO VIEW

The top tier, the Equipment Tier, is a diverse collection of test equipment, threat/vulnerability information sharing databases, simulation, and development equipment groups. The center tier, the Infrastructure Tier, is composed of networking, data storage, and the servers and devices supporting the other tiers. The bottom tier, the Interfacing Tier, provides for distribution of the ACATS across rooms, floors, buildings, and hosted environments whether virtualized in macro or micro pieces, and provides constricted access to desktops, vendors, academia, law enforcement, and other entities. The base on which the ACATS is built is the Infrastructure Tier.

3.2 INFRASTRUCTURE TIER

Virtualization and the movement of large data blocks are important functions of the Equipment Tier. Figure 3 presents a high-level view of the Infrastructure Tier.

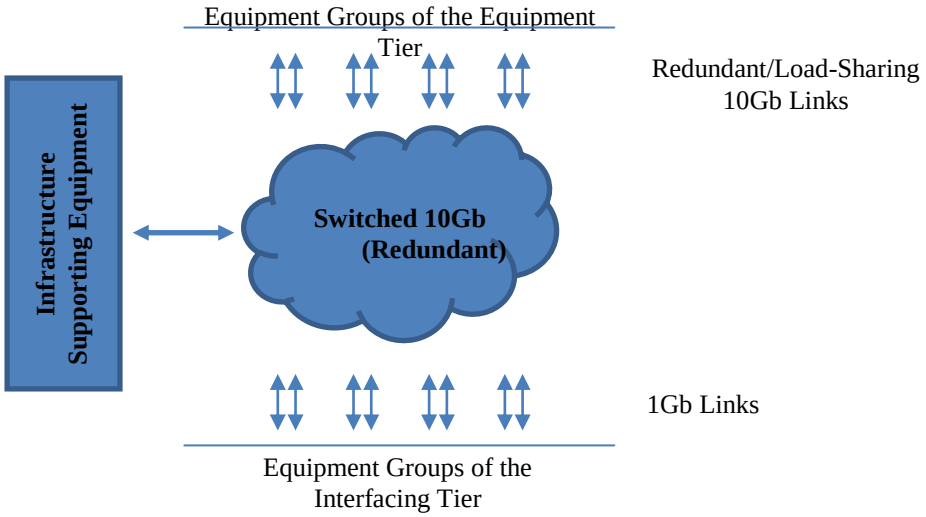


FIGURE 3. INFRASTRUCTURE TIER

The basis of this tier and its coupling to the other tiers is IPv6 with support for IPv4, the reverse of the traditional infrastructural implementation of these protocols across a network fabric. The purpose of this strategy stems from IPv4 as the primary protocol used by aircraft systems, as defined by Aeronautical Radio Incorporated (ARNIC) standards for LRUs. It often happens in test and development environments where the tester/developer modifies his routing and addresses tables with the result of inadvertent disconnection from the infrastructure, thereby turning his environment into an inaccessible island and requiring out-of-band means, such as server console access to restore connectivity, usually by rebooting.

Substantially reducing this problem occurs by basing the ACATS infrastructure fabric on IPv6, because manipulation of IPv4 spaces has no effect across the fabric. However, there are devices and systems that do not support IPv6; some support of IPv4 is required. Other advantages of IPv6 across the infrastructure fabric include:

- IPv4 packets leaked from penetration tests have nowhere to go, such as into other test environments or corrupting the infrastructure; and,
- Packets external to the ACATS, such as the Internet, have nowhere to go except to proxy specific services.

Additionally, we propose that no packets (both IPv4 and IPv6) within the infrastructure fabric have a default route to external interfaces and must instead, use proxy services thereby adding a second layer of leakage protection. Figure 4 depicts infrastructure routing. Substantial data storage requirements accompany the Equipment Tier, as broadly outlined in the following sections.

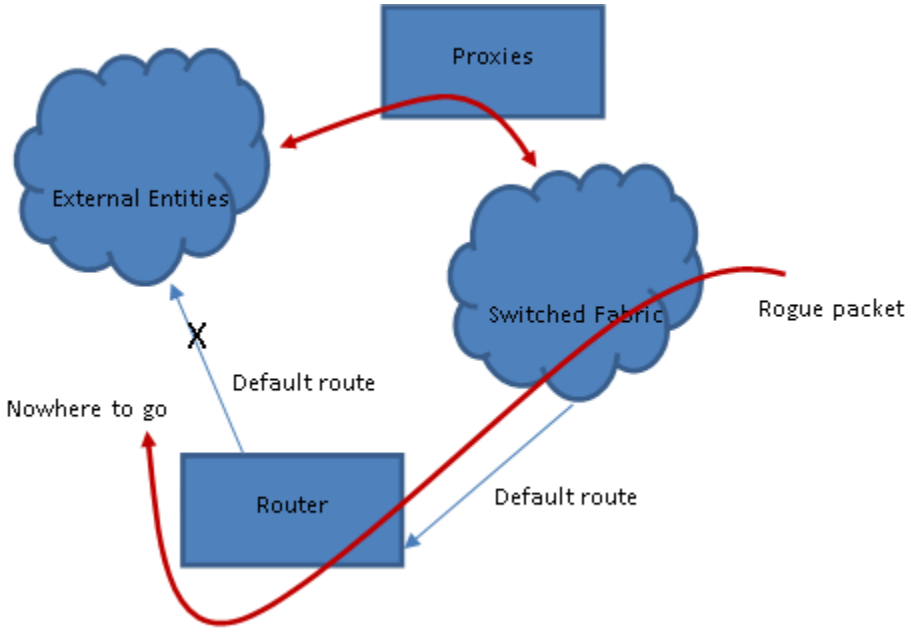


FIGURE 4. ROUTING INSIDE/OUTSIDE

3.2.1 VIRTUALIZATION STORAGE

The two common approaches of providing storage for virtualized instances are local and network storage over the Internet Small Computer System Interface (iSCSI) and the Network File System (NFS) protocols. There are tradeoffs to both approaches, including:

- Local storage capacity and technology is limited compared to networked storage.
- Long delays and performance degradation when moving an instance within a cluster (e.g., vMotion) across local storage, whereas network storage simply requires disconnection from one server and reconnection to another
- Hardware failure of servers using local storage incurs long recovery times (e.g., system rebuild and restoration, and awaiting arrival of maintenance personnel or parts).
- Diverse latency (e.g., network storage may be fronted by large caches).
- Snapshotting of instances (i.e., backup) forces an instance off-line for the duration whereas a snapshot of an iSCSI disk hosted on a ZFS[1] pool is near instantaneous (i.e., ZFS supports copy-on-write)[2].

Network storage, such as ZFS pools are chunked and presented as "disks" to a virtual server over iSCSI[3] whereas local storage is chunked from collections of 500GB RAID1 disks, or partitioned from a larger RAID array. Whereas networked storage can be provided by variable sized chunks spread across arrays of "spindle sets" (i.e., physical disks), by comparison local storage structures are static. Consequently, balancing load across static structures is more difficult and constrained than balancing across network storage. Additionally, network storage technologies often fronted by large amounts of RAM and SSD caches yield near instantaneous response, whereas the application of caching strategies is limited with local storage.

In both network and local storage, contention locking is at the logical unit number (LUN). When a large array partitioned into disks on a virtual server is then further partitioned into virtual disks to instances, significant performance bottlenecks arise as more instances share the LUN.

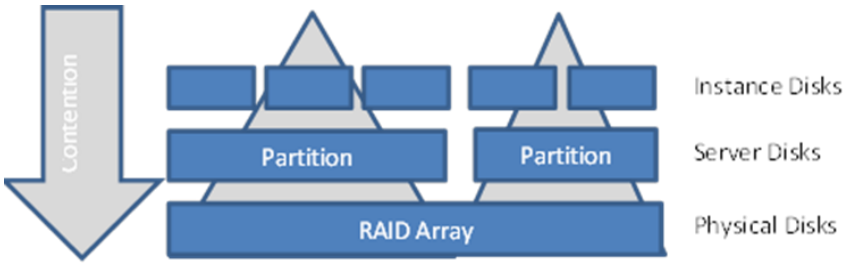


FIGURE 5. LOCAL STORAGE STACK

[1] Zettabyte File System. http://en.wikipedia.org/wiki/ZFS

[2] The tradeoffs between a VMware instance snapshot and a ZFS snapshot are significant. For example, a ZFS snapshot does not include hypervisor and instance in-memory disk blocks.

[3] VMware's NFS protocol implementation is notoriously slow and iSCSI interfaces often include hardware assist.

A key difference between network and local storage comes back to VMWare's vMotion. With local storage, an instance reads from one array, is transported over the network, then written onto to another array. This process creates read contention on the first virtual server, writes contention on the second, and consumes network bandwidth. These contention points can have significant, negative impacts on other instances sharing the arrays, whereas with network storage there is less contention: logical connections from the first virtual server move to the second. In either case however, there is overhead of block flushing on the first server and startup costs on the second.

From a LUN perspective, we propose to provide 100-250GB LUNs across several 8TB[4] RAIDz2 pools (spindle sets) to the virtual servers over iSCSI. The ACATS proposes support for 35 virtualized servers with eight to sixteen network LUNs each, or roughly 35*16*250GB=140TB of storage. Additionally, the smaller storage requirements of the Hypervisor itself (8-16GB) may be provided over iSCSI to offer snapshot/roll-back capability.

Local storage versus network storage is not an either/or choice, but rather, virtual servers are best served by a hybrid of those technologies. For example, it is always best to keep the hypervisor swap space and instance swap spaces local to the server itself. In addition, some operating systems (OS) simply cannot handle not being in direct contact with its disks, such as when their disk I/O timers are tuned to local hardware, and not to network abstractions with varying latencies.

3.2.2 ATTACKING HASHES

There are two dictionary approaches when attacking hashes: precompiled dictionaries, and active permutation operations against a base dictionary (i.e., in-attack word generation). These approaches, coupled with the attack tool (e.g., John-the-Ripper[5], Aircrack[6], and oclHashcat[7]), have significant time/space tradeoffs, including:

- Precompiled dictionaries have significant space requirements but near zero generator requirements, leaving the attack tool to focus on the computational aspects of encoding and comparing hashes.
- Multiple word permutation masks (e.g., run against Mask1, then against Mask2, and then against Mask3 – all different masks) often produce significant amounts of duplication thereby affecting attack efficiency.
- The implementation of the attack tool can dictate the dictionary source and consequently, one cannot get away from precompiled dictionaries.

The capability to attack hashes and cryptographic protocols in a cyber security and analysis environment is an important capability against cyber miscreants. For example, some gamer

[4] 5x3TB disks, RAIDz2 (RAID6), minus 10% ~= 8TB.

[5] http://www.openwall.com/john/

[6] http://www.aircrack-ng.org/

[7] http://hashcat.net/oclhashcat/

laptops (e.g., Alienware[8] -- PODs) have dual Radeon 290X GPUs capable of mounting formidable attacks against in-service, on-board cryptographically protected systems (e.g., wireless communications). Additionally, captured cryptographic transactions can be attacked off-line, potentially yielding active keys. The hash attack capabilities available to ordinary persons are very formidable. The following URL depicts an individual's system that can attack an NT LAN Manager (NTLM) hash at a rate of ~130 giga-hashes per second.

- http://hashcat.net/forum/archive/index.php?thread-2587.html

The mechanics of attack tools widely vary. For example, some tools support UNIX pipes where a compressed dictionary can be fed from a decompressor, then into the tool such as:

```
pbunzip2 --decompress --stdout /NFS/length_10.sorted.bz2[9] | john …
```

Other tools require access to the dictionary itself, but do not support decompression (e.g., Aircrack). In these and other cases, it is often desirable to chunk the dictionaries for better load distribution and failure recovery, such as when using MPI[10].

This proposal includes storage for precompiled dictionaries. One existing dictionary, the author's dictionary, consumes 57TB when uncompressed, and 8TB in its highly compressed form[11]. Adding storage for other precompiled dictionaries such as rainbow tables, database provision mechanics, and manipulation of large files requires an estimated storage of 250TB.

3.2.3 VERSIONING

Versioning is the broad implementation of maintaining versions of virtualized instances, software libraries (including LRU loadable parts), operating system DVDs (e.g., Kali, CentOS, etc.), and software development tools. It is expected that on-line versioned digital objects (i.e., collections of items) will remain for approximately one year before first being committed to an on-line archival system, and then to an off-line archival system. The estimated storage requirement is 100TB.

3.2.4 INFORMATION SHARING

It is difficult to estimate the storage requirements of information sharing systems without some idea of mechanics and content. We assume there will be significant content backed by databases but whose space requirements do not rival the ACATS's other infrastructure requirements. Consequently, the estimated storage requirement is 25TB.

3.2.5 SPACE REQUIREMENTS SUMMARY

The previous space estimations did not include many other elements including user home directories, logging, transition and manipulation spaces, TCPDUMP, log digesters, analytical

---

[8] http://www.alienware.com/

[9] This file is 517GB compressed and un-compresses to >10TB.

[10] Message Passing Interface. http://en.wikipedia.org/wiki/Message_Passing_Interface

[11] Between 83% and 87% compression.

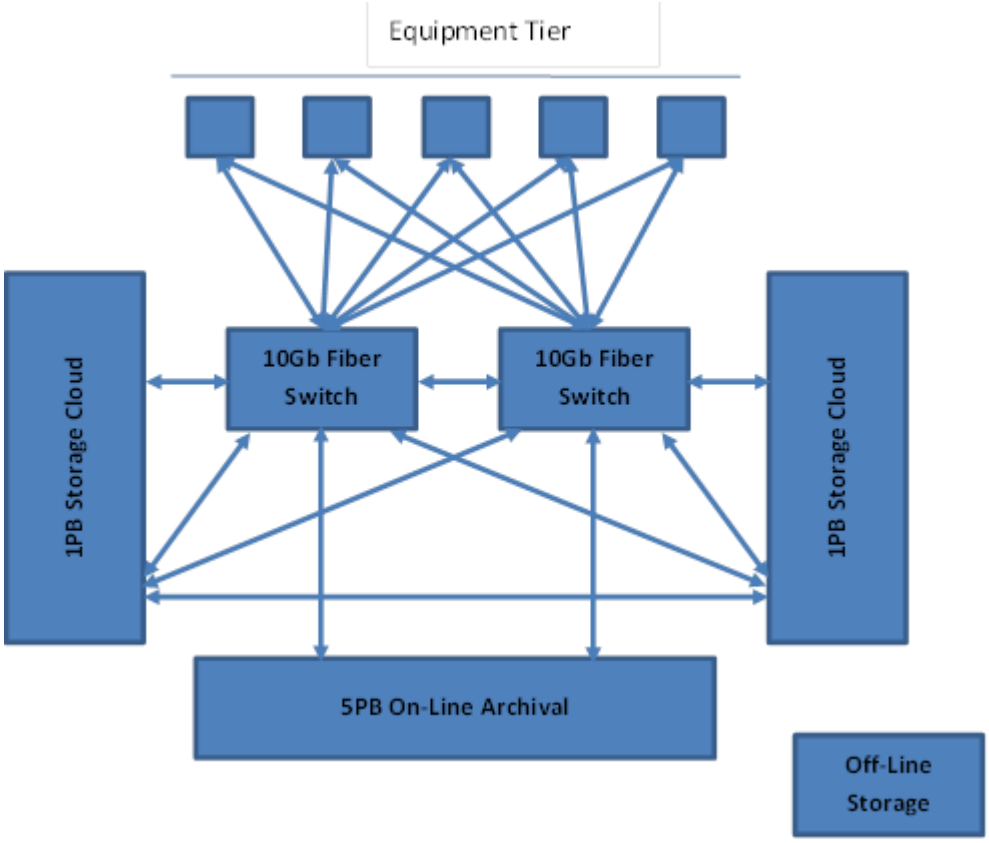
tools (e.g., Splunk[12]), and segmentation requirements, to name a few. Consequently, we propose to round up the space requirements from 515TB to 1PB.

3.3 ADDITIONAL INFRASTRUCTURE TIER DETAIL

Additional requirements of the Infrastructure Tier include network and data redundancy and high availability. Implicit in these requirements is load distribution. Figure 6 shows two (2) 1PB data clouds to provide mirrored redundancy and load distribution to the Equipment Tier, with an additional 5PB of dense storage for two to three years of on-line archives before commitment to off-line storage.

The use of fiber across the infrastructure fabric provides the capability for tier components to not be collocated, such as a 1PB storage cloud, and the 5PB cloud collocated in a data center, and the second 1PB cloud (or mirrored subsets) closer to the Equipment Tiers, which themselves may be physically distributed (See Section 3.13).

Not shown in figure 6 are other infrastructure support elements including two "services servers", two virtual servers, a router, and other devices. The services servers run on bare metal to boot the tiers and run services across (e.g., domain name system (DNS)). The virtual servers provide redundant sets of services often supplied as virtualized appliances, such as VMware's vCenter and authentication and certification services (e.g., Active Directory (AD)). Other services, such as network management, could run on the services servers or the virtualized servers.



[12] http://www.splunk.com/

FIGURE 6. INFRASTRUCTURE TIER NETWORKING AND STORAGE

3.4 INTERFACING TIER

The Interfacing Tier is composed of devices, such as Juniper SSG-140s to interface the ACATS to external entities and infrastructures such as the Internet, VPNs to vendors and academia, and governmental agencies. As such, this tier is simple and straight-forward.

An example of how the ACATS extensions would work is if an academic research project were hosted in the Amazon Cloud (EC2[13]), and its rehosting into ACATS was infeasible. Creating a VPN between the research project and ACATS would restrict its reach within the ACATS but provide necessary access and services.

3.5 EQUIPMENT TIER

The Equipment Tier is the most complex and diverse of the three tiers. Its major elements are "equipment groups" for the logical grouping of their purpose such as penetration testing, and simulation. The base architecture of an equipment group is straight-forward and depicted in figure 7.

An equipment group connects to the Infrastructure Tier through a 10Gb switch with 10Gb and 1Gb connections to the group's devices. For example, making a 10Gb connection to each group's servers to support bulk data transfer to the Infrastructure Tier, and to localize traffic within the group itself (e.g., vMotion), thereby reducing the aggregate contention and traffic within the Infrastructure Tier that would otherwise have a negative impact across all equipment groups, such as virtual distributed switch (VDS) latency. Unlike the Infrastructure Tier, the only redundancy within an equipment group is from the grouping of virtualized servers into a cluster – there is no intra-group network redundancy.

An interesting aspect of equipment groups is the potential of logically grouping groups for larger projects, and the subdivision and reassignment of pieces to other groups. For example, two simulator groups, each providing an airport with multiple airlines and their back offices logically grouped with a penetration group for coordinated attack, such as a DoS across them, or an on-loan device interfaced to one group then reconnected to another.

As we will show across the following sections, pieces are pieces. Specifically, when a physical device is manufactured into a logical device, or "virtual object," that object may reside anywhere, such as collocated with an equipment group, an equipment bench in a room above you, or within a manufacturer's facility. Logically then, that object resides somewhere within a greater cloud, and its physical location relatively unimportant. This physical disassociation of objects into the cloud also provides for object connectivity to research projects such as next generation avionics systems (See Section 3.13).

[13] http://aws.amazon.com/ec2/

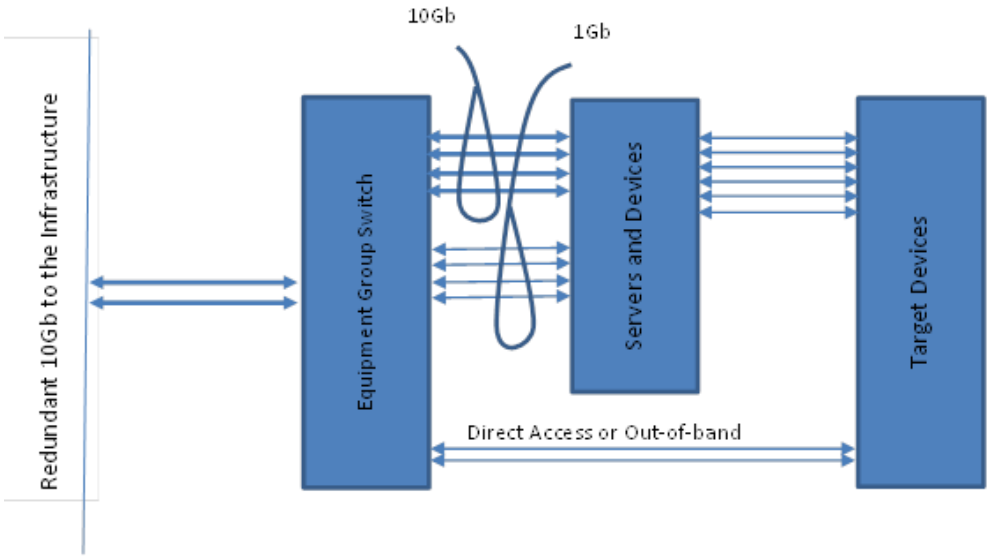


FIGURE 7. HIGH-LEVEL DEPICTION OF EQUIPMENT TIER

3.6 VIRTUAL AND OTHER SERVICES

The common server building block across equipment groups is a blade of seven or more servers. Typically, three to five servers compose a virtualized cluster and another two servers are netbooted (i.e., they are "bare metal"). Normally inaccessible under hypervisors, the bare metal servers may include wireless transceivers, Ethernet ports for direct manipulation by a customized kernel for special effects, and GPU accelerators for active, in-line man-in-the-middle (MITM) cryptographic attacks.

3.7 TEST EQUIPMENT GROUP AND HARDWARE IN THE LOOP INTERFACING

The purpose of the Test Equipment Group is a direct interface to LRU hardware, such as a FMS. In this group, the virtual servers:

- Provide emulation services to LRU software (i.e., the actual LRU software itself – its BIOS, its OS, and its applications).
- Provide localized environments for penetration tool sets and attack scenarios.
- Provide localized test-specific and airline backend services, such as loadable part signing and staging, AMI generation, certification, and transport across a simulated airport/MRO infrastructure onto an aircraft[14].

Expander switches (e.g., a Cisco 3850) whose ports are VLANed to interfaces of the units under test (UUT), provide Ethernet connectivity from the virtualized servers to the LRUs. Technologically speaking this is straight forward however, a novel approach is required to interface analog/digital (A/D) converters, general purpose input/output (GPIO), and displays, to name a few interfacing technologies to ACATS.

[14] See **Error! Reference source not found.**

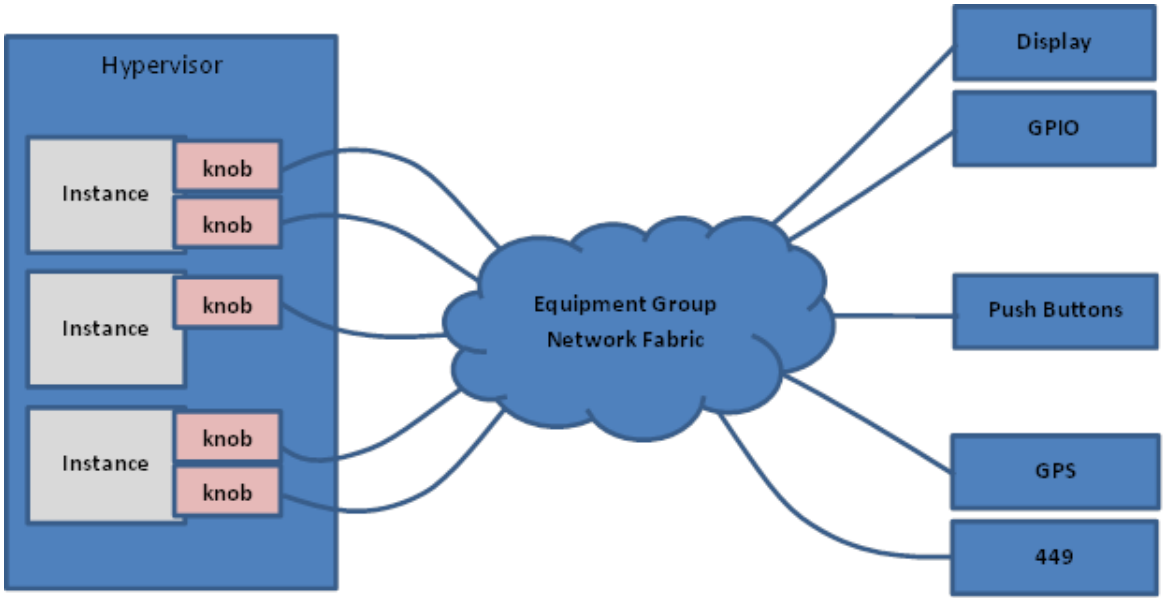


FIGURE 8. BEAGLE BOARD EXPANDERS

Figure 8 illustrates LRU software encapsulated into virtualized instances with knobs written into the hypervisor to provide emulated interfaces, such as GPIO and digital/analog conversion. These knobs translate manipulation by an attached instance into a generic protocol across a TCP connection to a Beagle Board[15] or ZedBoard[16], which interprets the generic protocol into an action on a "cape", such as a touch screen[17], Global Positioning System (GPS)[18] , or an RF transceiver[19]. This coupling could further be reduced from logical to physical interfaces to logical to logical interfaces, as depicted in Figure 9.

Implicit in this "pieces are pieces" approach, or the "decomposition" of physical associations into the logical and virtual associations, is that interconnected entities do not have to exist within the same space. Rather, they can be physically disjointed, such as the components of Cloud A located at a secure facility, and Cloud B located at an academic research project in Amazon's EC2.

We are proposing the incremental decomposition of aviation components into virtualized objects where these objects exist somewhere within logical spaces (i.e., arbitrary "cloud" boundaries) for the purpose of cyber security testing and research. It is our hope ACATS may someday extend into a foundational project where LRU components could exist within a cloud onboard an aircraft, thereby reducing aircraft complexity and weight with substantial operating savings and environmental benefits.

---

[15] http://www.beagleboard.org

[16] http://www.zedboard.org/

[17] http://elinux.org/CircuitCo:BeagleBone_LCD7

[18] http://elinux.org/Beagleboard:BeagleBone_GPS/GPRS_Cape

[19] http://elinux.org/CircuitCo:BeagleBone_RF

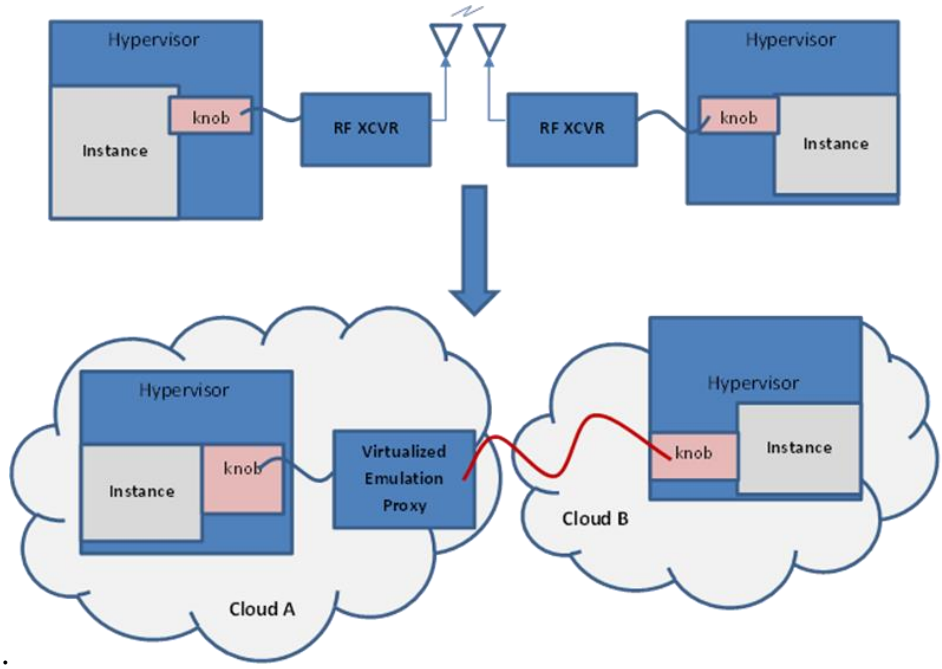


FIGURE 9. MIGRATION FROM THE PHYSICAL TO THE VIRTUAL

3.7.1 BEAGLE BOARDS

In addition to providing extended input/output (I/O) capability to an emulated LRU, Beagle Boards could provide the capability for interesting penetration approaches. For example, a Beagle Board providing a radio frequency (RF) connection to an ACARS transceiver could fabricate messages or "fuzz" messages (e.g., PeachFuzzer[20]) in an attempt to corrupt aviation systems attached to the ACARS transceiver or the transceiver itself. Novel and interesting, there are two important things to keep in mind about this approach.

Advantage	Sophisticated interfacing technologies with complex support requirements and limited availability (e.g., a terminal wireless LAN unit (TWLU)), may be distilled into a cape for penetration testing.
Disadvantage	Specific technology expertise may be required to develop some capes, such as knowledge in RF circuit building. However, this expertise may be available in the form of interns and graduate students.

3.8 TEST SUPPORT EQUIPMENT GROUP

The Test Support Equipment group is a collection of one-of-a-kind and expensive devices, such as a Mu[21]. These devices, to the extent possible, will be networked into the Equipment Tier (i.e.,

[20] http://peachfuzzer.com

[21] Now owned by Spirent, "Mu" is a well-known technology name but the product line has been replaced. See http://www.spirent.com/Ethernet_Testing/Platforms/C100_Chassis

they are objects with the logical cloud) but physical breakouts will also be provided, shown in Figure 10.

This group includes a liquid cooled, multi GPU server for use in off-line crypto attacks, such as passwords, wireless pre-shared keys (PSK), and secures protocols. This server, likely running oclHashcat and John-The-Ripper[22] would provide the following capabilities:

- Provide evidence to the contrary to those who assure their passwords/PSKs are well chosen.
- Provide evidence to the weakness of PSK choices. Even today with a mountain of articles and examples to the contrary, people refuse to believe the vulnerabilities of their PSK choices until presented with conclusive evidence.
- Facilitate brute-force attacks against secure protocols.
- Recover cryptographic keys from compromised systems as part of its threat analysis, which could look like:
    - Short the power/ground pins of a USB interface causing the 22 device to power cycle,
    - Install an alternate OS on a memory stick and interrupt the device's boot process forcing it to boot from the stick,
    - Copy (e.g. using the UNIX dd command) the LRU's disk recovering /etc/shadow, and then,
    - Submit/etc/shadow to oclHashcat.
- A data recovery service of data encrypted for extortion purposes.

Other equipment that could be part of this equipment group includes Ethernet, spectrum, and other analyzers, as well as wireless, Bluetooth, and other penetration appliances.

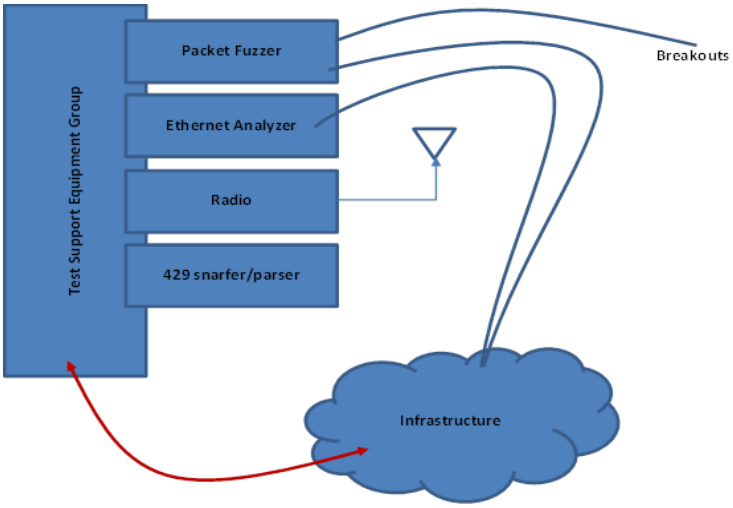


FIGURE 10. TEST SUPPORT GROUP

[22] JTR's "bleeding edge" version offers GPU acceleration through OpenCL.

3.9 THREAT ASSESSMENT EQUIPMENT GROUP

The Threat Assessment Equipment Group is a collection of servers providing databases, web servers, and other threat analysis (e.g., Splunk) collection, classification, and dissemination methods and technologies.

3.10 SIMULATION EQUIPMENT GROUP

The Simulation Equipment group is a large collection of servers providing the bulk of the virtualization across the Equipment Tier. It hosts clouds, macro and sub clouds, partial and dispersed clouds, interconnected objects across clouds, operational fabrics (e.g., the network schematic of a 747), and any other aviation assets that can be realistically reduced into virtualized objects into virtual environments. Some of these environments will be stable whereas others volatile.

The simulation equipment group also provides the versioning of objects, such as the loadable software and the configuration of a particular aircraft across a ten-year span. This versioning would allow for the cyber analysis of an in-service aircraft or similar in-service configurations, or the impact of a specific LRU vulnerability across multiple aircraft models.

The Simulation Equipment Group would support a description language (yet to be developed) that constructs objects then interconnects them. To whatever their extent, these objects would be packaged into blobs and stored in the archives. Expectations are that a blob could have significant storage requirements.

3.11 DEVELOPMENT GROUP

The Development Equipment Group is a collection of servers that are merely tools for penetration assessment techniques and simulated environments. The key difference between this group of servers and others is it is an unstable, volatile area.

3.12 SOFTWARE

We propose the evaluation of the “open source” simulation and aircraft simulation models, and modules against COTS simulation providers as the cost to develop, maintain, and evolve them would be prohibitive. The next phase of work should identify, evaluate, and select the simulation basic code foundation. This includes such items as:

- Foundation OS
- Bootstrap loaders
- Virtual data/network bus
- Simulation adapters (for connection/use of independent industry or university modules)
- Visualization systems (cockpit displays and simulation displays)
- Virtualization OS/s to run the actual aircraft simulation and modules
- VM management system
- VM configuration manager
- Data storage and movement manager
- Simulation authentication and authorization system/s

- Encryption systems (if required)

3.13 DECOMPOSITION

Explicit in the ACATS architecture, is the ability to physically disassociate aviation assets, or to "decompose" systems. A cockpit, for example, is a collection of physically collocated LRUs – they have to be physically collocated to fly the aircraft. A collection of LRUs does not exist in isolation and must have a supporting infrastructure, such as for data loading and configuration. The interconnection requirements across LRUs and the supporting infrastructure services are a substantial impediment to cyber security RDT&E. For example, to test an ARCARS LRU a connection to other LRUs must exist, and there must be an external HF transceiver sending and receiving ACARS messages.

Using Beagle Boards, Zed Boards, and custom hardware as extenders, an LRU can exist physically disassociated from its connectivity and supporting infrastructure services because it would remain logically connected to them. Conceptually, GPIO, 429/629, and other LRU hardware interfaces form a network of sorts. The extenders simply convert from one network (e.g., 429/629) into another – Ethernet and IP packets. Extenders then, logically connect the physical LRUs into a working cockpit for physical dispersion across the US. This means, for example, an MIT researcher working on a next generation navigation system would have access to other LRUs and supporting infrastructure services without the burden of physical collation and its expense. In other words, the cockpit is "decomposed".

Currently, academic research and cyber security testing is limited by the burden of connectivity and support requirements. With decomposition and support services provided by ACATS, these and other activities could reach an explosive new level to the advancement of aviation.

As in all things, however, nothing is free. For example, some LRUs have timing requirements across them. Despite minimizing or mitigating these requirements by network technologies such as Multiprotocol Label Switching (MPLS), or through Service Level Agreements (SLAs), decomposition cannot be a complete substitute when a physical wire is required. Nonetheless, many LRUs do not have these requirements and ACATS with extenders can provide substantial benefits to collaborative cyber security testing and research and development.

4. CONCLUSIONS

From research, no open source or COTS aircraft simulators exist with cyber testing capabilities today. There may be some proprietary non-disclosed systems operated by airframers or their suppliers; classified non-disclosed systems do exist. Thus, we are proposing an aircraft cyber analysis and threat test-bed (ACATT) that merges "virtualized flight simulator" architecture with aircraft cyber security testing capabilities.

We recommend starting with an evaluation of the NASA Goddard open source (e.g. NASA/GSFC's Flight Software Core Flight System Report) as a foundation for the simulation software foundation, followed by reviews of several other "open source" simulation collections available

Once the foundational simulation is established, the FAA will be able to establish a capability and functional matrix of the desired cyber test capabilities and their priorities. From this matrix, follow-on work can evaluate the actual aircraft simulators, system modules, and cyber test suits to provide optimized recommendations for ACATS simulator functionality, maintainability, and cost. Likewise, with a defined foundation and established functional capabilities and priorities, long-term planning can begin for the incremental hardware growth required to host ACATS as it grows in capabilities.

We recommend the near term development of a proto-type with basic cyber test capabilities. Its development can employ minimal hardware, open source modules, and cloud-based storage and computing for cyber simulation testing of legacy aircraft. Functionality could include ACARS, FANs, or VDL-2 link cyber testing, and simulation of loadable software threat vectors. The prototype would also be invaluable to develop the FAA's vision for long-term cyber threat, test capabilities, and the associated hardware and software.

Cyber threat risk evaluations must become a specific, defined component of the aircraft's architecture, design processes, manufacturing, maintenance procedures, and operational guidance. Like any other aircraft component, adding something late in the design process may induce risks that not easily mitigated, or in worst case scenarios, may result in reduced aircraft functionality (i.e., may not be securable to a level to fully participate in NextGEN). Likewise, risk evaluations must be instantiated in maintenance procedures and operational guidance to ensure its continued airworthiness. As the aviation community currently expects and accommodates changes in operational experience and procedures, physical and environmental threats, and aircraft maintenance, there is a need to expect and accommodate the dynamic nature of cyber threats and vulnerabilities and their impact on safety. The ANSS testbed can provide critical assistance to both the FAA and industry in the assessment of aircraft cyber risks by provide ATG communications simulations of both abnormal communications/events and directed penetration or denial of service attempts.

5. REFERENCES

1. Zettabyte File System. Retrieved June 15th , 2014 http://en.wikipedia.org/wiki/ZFS

2. John the Ripper password cracker. Retrieved June 15th , 2014, from http://www.openwall.com/john

3. Heartbleed vulnerability and Aircrack-ng. Retrieved June 15th , 2014, from http://www.aircrack-ng.org/

4. Retrieved June 15th , 2014, from http://hashcat.net/oclhashcat

5. Amazon EC2. Retrieved June 15th , 2014, from http://aws.amazon.com/ec2/

6. Meet the Beagles: Open Source Computing. Retrieved June 15th , 2014, from http://www.beagleboard.org

7. CircuitCo:BeagleBone LCD7.Retrieved June 15th , 2014, from http://elinux.org/CircuitCo:BeagleBone_LCD7

8. CircuitCo:BeagleBone LCD7.Retrieved June 15th , 2014, from http://elinux.org/Beagleboard:BeagleBone_GPS/GPRS_Cape

9. CircuitCo:BeagleBone LCD7.Retrieved June 15th , 2014, from http://elinux.org/CircuitCo:BeagleBone_RF

10. Peach Fuzzer (2013). Retrieved June 15th , 2014, from http://peachfuzzer.com

11. "Mu" is a well-known technology name but the product line has been replaced. Retrieved June 15th , 2014 http://www.spirent.com/Ethernet_Testing/Platforms/C100_Chassis

12. McComas, David. (November 7-9, 2012). NASA/GSFC's Flight Software Core Flight System. Retrieved from http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20130013412.pdf

APPENDIX A—VENDOR WEB ADDRESSES

COTS Products Vendors	Web address
Cross-Simulator	http://cross-simulator.com/
FlyElite	https://www.flyelite.com/
Project Magenta	http://www.projectmagenta.com/
Commercial Level Simulations	https://www.commerciallevel.com/index.php?id=58
Integrated Simavionics	http://www.isgsim.com/?page=home
Boeing	http://www.boeing.com/boeing/commercial/aviationservices/flight-services/simulator-services/software_modeling.page
GEFS	http://www.gefs-online.com/
FlightSim	http://www.flightsim.com/
Flyanairliner	http://www.flyanairliner.com/products/flight-/
iAircraft	http://www.adi.com/products/iaircraft/
SimCheck International	http://www.simcheckinternational.com/simulators.html
Shareware sites	http://www.2000shareware.com/downloads/commercial/aircraft/simulators/ http://www.winsite.com/aircraft/aircraft+simulator+software/index3.html
Government Laboratories	**Web address**
NAWCAD	http://onroutreach-summer-faculty-research-sabbatical.com/naval_air_warfare_center_aircraft_division.html
NASA	http://www.aviationsystemsdivision.arc.nasa.gov/facilities/cvsrf/747_sim.shtml
USAF	http://www.jsf.mil/program/prog_field_wpafb.htm
University Laboratories	**Web address**
Virginia Tech College of Engineering - Vehicle and Aircraft Research Simulation Lab	http://www.ise.vt.edu/ResearchFacilities/Labs/LabPages/VARS_lab.html
Institute of Aviation, University of Illinois at Urbana Champaign	http://www.aviation.illinois.edu/avimain/index.php?option=com_content&view=article&id=33&Itemid=123

COTS Products Vendors	Web address
University of Toronto Institute for Aerospace Studies	http://www.utias.utoronto.ca/research/vehicle-simulation
West Virginia University Aircraft Simulation Laboratories	http://www.cemr.wvu.edu/research/center-details.php?&id=89&type=lab
University of Maryland Eastern Shore Engineering Program	https://www.umes.edu/Engineering/Default.aspx?id=26066
University of Tennessee Space Institute	http://www.utsi.edu/academics/avsys/research.htm
Wichita State University National Institute for Aviation Research (NAIR)	http://www.niar.wichita.edu/coe/cgar.asp
Embry-Riddle Aeronautical University Daytona Beach	http://daytonabeach.erau.edu/college-aviation/flight/simulation-training-devices/index.htm
University of North Dakota John D. Odegard School of Aerospace Sciences - Flight Operations	http://flightops.aero.und.edu/Facilities/ryanhallsimbay.aspx
En Route Integration and Interoperability Facility (EIIF)	http://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc/about/campus/faa_host/labs/csi_team/eiif/
Oceanic Integration and Interoperability Facility (OIIF)	http://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc/about/campus/faa_host/labs/csi_team/oiif/
NextGen Integration and Evaluation Capability (NIEC)	http://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc/about/campus/faa_host/labs/csi_team/niec/
Research Development & Human Factors Laboratory (RDHFL)	http://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc/about/campus/faa_host/labs/csi_team/rdhfl/
Florida NextGen Test	http://www.faa.gov/about/office_org/headquarters_offices/ang/of

COTS Products Vendors	Web address
Bed (FTB)	fices/tc/about/campus/faa_host/labs/csi_team/ftb/
NASA/GSFC's Flight Software Core Flight System Report	http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20130013412.pdf