A SECURITY RISK ANALYSIS OF THE DATA COMMUNICATIONS NETWORK PROPOSED IN THE NEXTGEN AIR TRAFFIC CONTROL SYSTEM

By

ROBERT G. WOOD

Bachelor of Science in Network Management
Southern Nazarene University
Bethany, OK
2002

Master of Science in Information Technology
University of Texas
San Antonio, TX
2006

Submitted to the Faculty of the
Graduate College of
Oklahoma State University
In partial fulfillment of
the requirements for
the Degree of
DOCTOR OF EDUCATION
May, 2009

A SECURITY RISK ANALYSIS OF THE DATA

COMMUNICATIONS NETWORK

PROPOSED IN THE NEXTGEN

AIR TRAFFIC CONTROL

SYSTEM

Dissertation Approved:

Dr. Mary Kutz
Dissertation Adviser, Committee Chair

Dr. Lynna Ausburn
Committee Member

Dr. Timm Bliss
Committee Member

Dr. Steve Marks
Committee Member

Dr. A. Gordon Emslie
Dean of the Graduate College

ACKNOWLEDGMENTS

This is perhaps the most difficult page of the study to develop. It is not easy to know where to begin thanking the many people who have contributed directly and indirectly to my research. I thank God for those who have been placed in my path at just the appropriate instant during my life and my studies including my parents, Carl & Sylvia Wood (Cunningham), who set an early example of hard work and sacrifice; my wife Nita, who has both supported and tolerated the lifestyle of a perpetual student; and my son Christopher, who always makes me laugh while juggling family, career, and academic pursuits.

I deeply appreciate the members of my committee for making the investment of time and contributions to this work while guiding me through the dissertation process. I would particularly like to thank Dr. Mary Kutz for her wise counsel throughout the Aviation & Space Science degree program, and for allowing me to use her as a sounding board for new concepts and ideas. The relationships that have grown out of this program within the academic community, with other students, and resultant professional networks are priceless. I can only hope to serve others going forward in the same manner that this program has served me.

TABLE OF CONTENTS

Chapter Page

I. INTRODUCTION 1

Statement of the Problem 3
Purpose of the Study 3
Research Questions 4
Definition of Terms 5
Significance of the Study 10
Assumptions 11
Limitations 11
Theoretical Framework 12
Organization of the Study 13

II. REVIEW OF LITERATURE 15

Introduction 15
NextGen Active Network: ADS-B 16
NextGen Features and Concepts 17
NextGen Network 24
Known Concerns with ADS-B security 27
Computer Network Security Best Practices 29
Cisco Systems Changed Threat Landscape 30
Microsoft Security Development Lifecycle 31
Government Standards and Industry Best Practices 32
Summary of the Literature Review 36

III. METHODOLOGY 37

Introduction 37
Research Design 37
Selection of the Sample 38
Instrumentation and Procedures 41
Data Analysis 43

Chapter Page

IV. FINDINGS....44

Introduction....44
Sample Depth of Knowledge....45
Confidentiality....47
Participant #1....47
Participant #2....49
Participant #3....49
Participant #4....50
Participant #5....51
Participant #6....52
Integrity....54
Participant #1....54
Participant #2....55
Participant #3....55
Participant #4....56
Participant #5....59
Participant #6....60
Availability....62
Participant #1....62
Participant #2....63
Participant #3....63
Participant #4....65
Participant #5....67
Participant #6....68
Additional Comments....70
Participant #1....70
Participant #2....71
Participant #3....71
Participant #4....72
Participant #5....72
Participant #6....74
Thematic Analysis of Participants....76
Confidentiality....76
Integrity....77
Availability....78
Financial Impacts....80
Government, Industry & Education Partnerships....81

Chapter Page

V. CONCLUSIONS AND RECOMMENDATIONS 83

Conclusions 83
NextGen Comparison to Network Security Standards 84
NextGen Performance Against Common Threats 86
NextGen Compliance with FISMA Objectives 87
Security Recommendations 88
Final Recommendations 90
Future Research 91
Final Conclusion 92

REFERENCES 93

APPENDICES 99

APPENDIX A - IRB APPROVAL FORM 100

APPENDIX B – INFORMED CONSENT FORM 101

APPENDIX C – INTERVIEW QUESTION GUIDE 104

APPENDIX D – SAMPLE ORGANIZATION APPROVAL LETTER 107

LIST OF TABLES

Table Page

1. Definition of Terms....5

2. Theoretical Perspective....13

3. Potential Security Impact Definitions....34

4. NextGen ADS-B Security Categorization....35

5. Participants by Discipline and Market Segment....40

6. Interview Procedures....42

7. Depth of Knowledge of Participants....45

8. Perspective Synopsis: Confidentiality....53

9. Perspective Synopsis: Integrity....61

10. Perspective Synopsis: Availability....69

11. Perspective Synopsis: Financial Impact....81

12. Perspective Synopsis: Government, Industry & Education Partnerships....82

LIST OF FIGURES

Figure Page

1. Triangulation Model 16

2. NextGen Functional Diagram 19

3. ADS-B Functional Diagram 20

4. Sample CDTI Display including weather 21

5. Sample Garmin ADS-B cockpit display including traffic and weather 22

6. Sample ADS-B ground traffic display 23

7. The Changed Threat Landscape 30

8. Security Development Lifecycle 31

CHAPTER I

INTRODUCTION

Over 750 million aviation passengers were carried in the United States during 2006 (JPDO, June, 2007). By 2012 to 2015 that number could exceed one billion. The existing air traffic control system cannot adjust to the current and anticipated growth in aviation traffic. NextGen is the Federal Aviation Administration's term for the next generation air traffic control system. The planned system is a wide ranging transformation of the entire national air transportation system to meet future demands and avoid gridlock in the sky and at airports. NextGen uses active networking technology which is tailored to the individual needs of users within the system. It moves away from legacy analog technologies and ground-based radar to new satellite and airborne digital data technologies. These new capabilities and the highly interdependent technologies that support them will change the way the system operates, reduce congestion, and improve the passenger experience (FAA, 2008).

The multi-agency NextGen initiative is led by the Joint Planning & Development Office (JPDO) and includes participation by the Department of Transportation, Federal Aviation Administration (FAA), Department of Defense (DoD), Department of Homeland Security (DHS), Department of Commerce (DoC), National Aeronautics & Space Administration (NASA), and the White House

Office of Science & Technology Policy, plus interested public, commercial and academic entities.

According to the Federal Aviation Administration (FAA, 2008), some of the benefits that NextGen brings to aviation include:

- Air-to-air surveillance capability
- Surveillance to remote or inhospitable areas that do not have radar coverage
- Real-time traffic and aeronautical information in the cockpit
- Reduced separation and greater predictability of departure and arrival times
- Common separation standards, both horizontal and vertical, for all classes of airspace
- Improved ability of airlines to manage traffic and aircraft fleets
- Improved ability of air traffic controllers to plan arrivals and departures far in advance
- Reduced cost of the infrastructure needed to operate the National Airspace System (NAS)

The positive effect on safety for portions of NextGen have already been proven in prototypes including the Automatic Dependent Surveillance – Broadcast (ADS-B) (Gardner, 2005, p. 115), ADS-B has been utilized for several years in field testing conducted in both Alaska and the Ohio River Valley. Additional studies have been undertaken to understand the potential benefits and incentives of ADS-B (Lester & Hansman, 2007). The FAA describes ADS-B as the backbone of the NextGen system.

While the potential safety, operational, and financial implications of NextGen are known, the underlying digital communications technologies utilized to produce these

benefits have not previously been used to monitor and control aviation. Data transmissions occurring between aircraft, ground monitoring stations, and satellites share risks common to the information flowing between computers over any digital network.

Statement of the Problem

The problem of focus for this research was the potential security risk imposed by implementing the active network technologies utilized by ADS-B in the NextGen air traffic control system, and more specifically the air-to-air, air-to-ground, and satellite-to-air links used by NextGen. Factors contributing to risk include interests both internal and external to the United States that could benefit from manipulating, impairing, or data mining the digital information being exchanged by aircraft and controllers. A risk analysis is needed of the ADS-B data network proposed for NextGen compared to industry best practices for system and network security. The NextGen system offers a wealth of improvements to national and international aviation safety, but may create unnecessary risks if the technologies used to implement the system do not include appropriate data and software security.

Purpose of the Study

The purpose of this study was to identify and describe the risks perceived by experts to be inherent to the active network within the ADS-B portion of the proposed NextGen system by comparing the enterprise architecture against current best practices in computer network security. Many of the evolving standards for computer network security have been developed through the efforts of information technology vendors including Cisco Systems and Microsoft. Additional groups have been formed to create

recognized industry certifications such the Certified Information Systems Security Professional (CISSP) and Certified Software Security Lifecycle Professional (CSSLP) from the International Information Systems Security Certification Consortium (ISC^2), and the Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute.

Many of the best practices and standards developed within the commercial sector have been codified within the public sector and have resulted in both legislation and government standards for network security. The National Institute for Standards and Technology (NIST) has also published a series of Special Publications which provide guidance for securing and assessing risk in computing systems. NIST publications of note for this study included the Risk Management Guide for Information Technology Systems (National Institute of Standards and Technology (U.S.), 2002a), and the Guide for Assessing the Security Controls in Federal Information Systems (National Institute of Standards and Technology (U.S.), 2006). Benchmark legislation was enacted in 2002 entitled the Federal Information Security Management Act (FISMA) (United States Congress Committee on Government Reform, 2003).

Research Questions

The primary questions that this study sought to answer were:

1. How does proposed ADS-B network design for the NextGen air traffic control system compare to government and commercial industry network security standards?

2. How does the ADS-B portion of the proposed NextGen network design perform when faced with common computer network threats such as Denial of Service, Session Hijacking, and Network Eavesdropping?
3. How does the ADS-B portion of the NextGen network model insure confidentiality, integrity, and availability?

Definition of Terms

The aerospace industry in general and NextGen in particular is rife with acronyms and special terms that describe the components discussed in this study. To assist the reader in deciphering this document and developing an understanding of the material a definition of terms and acronyms have been provided in Table 1.

Table 1.

Definition of Terms

Term	Description
802.11	Wireless computer network standard commonly found in homes, offices, and businesses like Starbucks
1090-ES	1090 MHz Extended Squitter. One of two data link technologies which are supported by the ADS-B portion of NextGen. 1090ES operates at 1090 MHz, and uses the Mode-S Extended Squitter standard common to SSR
ACSS	Aviation Communication and Surveillance Systems
ADS-B ARC	ADS-B Aviation Rulemaking Committee
ADS-B	Automatic Dependent Surveillance – Broadcast: NextGen uses 1090ES and/or UAT signals from vehicles to provide air traffic controllers and pilots with accurate position information and provide a real-time display of air or ground traffic
ADS-R	Automatic Dependent Surveillance – Rebroadcast

Term	Description
AGL	Above Ground Level
AIRMET	Airmen's Meteorological Information
ANSP	Air Navigation Service Provider
AOPA	Aircraft Owners and Pilots Association
ARC	Aviation Rulemaking Committee
ARTCC	Air Route Traffic Control Centers
ATC	Air Traffic Control
ATCRBS	Air Traffic Control Radar Beacon System
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
CAVS	CDTI Assisted Visual Separation
CDA	Continuous Descent Approach
CDTI	Cockpit Display of Traffic Information
CISSP	Certified Information Systems Security Professional
ConOps	Concept of Operations
CAN	Center for Naval Analyses and Institute for Public Research
CNA	Computer Network Attack
COI	Community of Interest
CPDLC	Controller Pilot Data Link Communications
CRC	Cyclic Redundancy Check
CSSLP	Certified Secure Software Lifecycle Professional
CTAF	Common Traffic Advisory Frequency
DER	Designated Engineering Representative
DME	Distance Measuring Equipment
DoD	Department of Defense (U.S.)
DoDAF	Department of Defense Architectural Framework
DoS	Denial of Service attack
DoT	Department of Transportation
DRM	Digital Rights Management
EFB	Electronic Flight Bag
EHS	Enhanced Surveillance

Term	Description
ELS	Elementary Surveillance
Eurocontrol	The European Organisation for the Safety of Air Navigation
FAA	Federal Aviation Administration
FAA Part 135	Commuter and On-Demand Air Carrier regulations
FEC	Forward Error Correction
FIS-B	Flight Information Service – Broadcast
FISMA	Federal Information Security Management Act
FMS	Flight Management System
GA	General Aviation
GBT	Ground Based Transceiver
GIAC	Global Information Assurance Certification
GNSS	Global Navigation Satellite System
GPS	Global Positioning System: determines a 4D position using satellites.
HFOM	Horizontal Figure of Merit
HPL	Horizontal Protection Limit
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
INS	Inertial Navigation System
IP	Internet Protocol
ISC^2	The International Information Systems Security Certification Consortium
ITT	ITT Corporation, prime contractor to the FAA for the development and deployment of ADS-B in the United States
IWP	Integrated Work Plan
JPDO	Joint Planning and Development Office: a partnership of agencies and stakeholders who are planning the NextGen air traffic control system.
MAC	Message Authentication Code
MAPS	Minimum Aviation System Performance Standard

Term	Description
METAR	Aviation routine weather reports
MFD	Multifunction Display
Micro-EARTS	Micro En route Automated Radar Tracking System
MIT	Massachusetts Institute of Technology
MLAT	Multilateration
MLS	Microwave Landing System
MOPS	Minimum Operational Performance Standards
MSL	Mean Sea Level
MVFR	Marginal Visual Flight Rules
Multilateration	or hyperbolic positioning, is the process of locating an object by accurately computing the time difference of arrival (TDOA) of a signal emitted from the object to three or more receivers
NACV	Navigational Accuracy Category for Velocity
NAS	National Airspace System
NEXCOM	Next Generation Air/Ground Communication
NEXRAD	Next Generation Weather
NextGen	Next Generation Air Transportation System
NIC	Navigational Integrity Category
NIST	National Institute of Standards and Technology
NOTAM	Notice to Airmen
NPRM	Notice of Proposed Rulemaking
NSA	National Security Agency (U.S.)
NTSB	National Transportation and Safety Board
NUC	Navigation Uncertainty Category
OAM	Original Aircraft Manufacturer
OV	Operational View
OV-3	Operational Information Exchange Matrix, as defined in DoDAF
PRM	Precision Runway Monitoring
PSR	Primary Surveillance Radar

Term	Description
RF	Radio Frequency
RNP	Required Navigational Performance
RTCA	Radio Technical Commission for Aeronautics or RTCA, Inc.: an organization which provides technical recommendations to the FAA comprised of over 335 members including foreign and domestic government agencies, airlines, airspace users, airport associations, labor unions, aviation service & equipment suppliers
SANS	SysAdmin, Audit, Network, Security Institute
SAMM	Surface Area Movement Management
SCAP	Security Certification and Authorization Package
SESAR	Single European Sky ATM Research Programme: the European version of NextGen
SFAR	Special Federal Aviation Regulations
SIGMET	Significant Meteorological Information
SIL	Surface Integrity Level
Spoofing	Any technique used to inject false or forged data into a network. In the case of NextGen this could be one or more non-existent vehicles, or altered location, speed, or timing data for an existing vehicle
SSR	Secondary Surveillance Radar
SUA	Special Use Airspace
TAF	Terminal Area Forecast
TAS	Traffic Awareness System
TAWS	Terrain Awareness and Warning System
TCAS	Traffic Collision and Alerting System
TCP/IP	Transmission Control Protocol / Internet Protocol
TDOA	Time Difference of Arrival
TFR	Temporary Flight Restriction
TIS-B	Traffic Information Service – Broadcast
Triangulation	uses a baseline and at least two angles measured such as with receiver antenna diversity and phase comparison
TSO	Technical Standard Order
TWIP	Terminal Weather Information for Pilots

Term	Description
UAT	Universal Access Transceiver
UHF	Ultra High Frequency
URET	User Request Evaluation Tools
UTC	Coordinated Universal Time
VDL	VHF Datalink
VFR	Visual Flight Rules
VHF	Very High Frequency
VMC	Visual Meteorological Conditions
VPL	Vertical Protection Limit
WAAS	Wide Area Augmentation System
WSI	Weather Services International
XM	Satellite-based weather and radar data service

Significance of the Study

Is the sky falling? This study will provide valuable information to determine the security risks surrounding implementation of the proposed NextGen air traffic control system. A study of this type should be extremely significant to many different groups which directly and/or indirectly utilize or could be impacted by air transportation. This study should be of interest to virtually the entire U.S. population who use products delivered by aircraft, fly for business or personal travel, or may be over flown by aircraft controlled by the system. The study should be of particular interest to the federal agencies comprising the Joint Program Development Office, non-governmental interests in the aerospace and transportation industries such as Boeing, Lockheed, Federal Express,

American Airlines, Honeywell, L-3, and other aviation manufacturing and transportation companies.

Unmanaged risks to the air traffic control system could result in flight delays, failed landings, mid-air collision, and other aviation disasters which would have potential impacts on passengers, pilots, crew members, ground personnel, and innocent bystanders.

Assumptions

A principle assumption made for this study was that adequate information regarding the design and security of the NextGen air traffic control system could be obtained through currently published enterprise architecture documentation, industry standards groups, and via interviews of engineering resources who are implementing the system within the various stakeholders.

Limitations

One limitation of this study was that most of the NextGen system had yet to be implemented, the enterprise architecture is to some extent still evolving, and the entire system would not be completed until roughly 2025. Some of these limitations, however, may also be advantageous as the outcomes of this study have the potential to positively impact the final implementation of NextGen security before it is completed, should significant risks be identified.

A second limitation of this study was the inability to obtain organization approval from each of the desired participants identified for the study. In two cases, approvals were withheld because the organizations were concerned that the information was too

sensitive to share in the open forum of a research study. In one additional case, the participants identified were unwilling to be formally interviewed or pursue organizational approvals for fear of career reprisals.

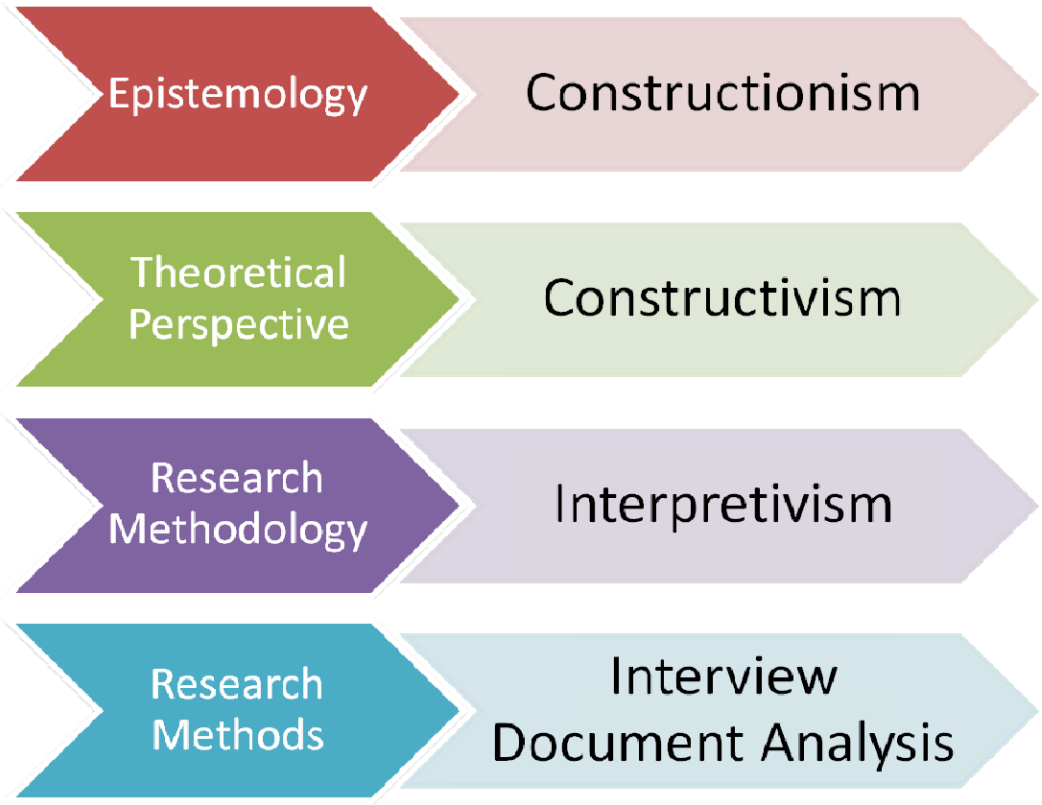
The participants for this study came primarily from the aerospace industry which restricted the scope of this research. The traditional design of qualitative research also limits the number of participants and restricts the ability to generalize results to the general population.

Theoretical Framework

The epistemology of the study was constructionism in that knowledge or truth was a product of consensus among selected participants in the context of the pertinent aerospace industry organizations. The theoretical framework used was constructivism which is a form of interpretivism in that it focuses on the experiences of the subjects interviewed and their direct lived experience. The methodology was a qualitative thematic analysis based on the study of existing design documents for the NextGen air traffic management system, computer security best practices, and interviews. Interviews were conducted and analyzed using a constant comparative method to arrive at emerging themes. In accordance with the characteristics of qualitative research, this study includes "clear and detailed descriptions of the study that includes the voices of the participants (Gay, Mills, & Airasian, 2006, p.402)." Table 2 shows the theoretical prespective utilized for this study.

Table 2.

Theoretical Perspective



Organization of the Study

Five main components were addressed in this study. The components include an introduction to the study, a review of available literature related to the security features within the proposed NextGen design, a methods section, a section on data collection and analysis, and a section of conclusions and recommendations.

The introduction includes a discussion of the need for this study as well as who will benefit from the information. An extensive set of terms is included for use against

literature reviewed and those used in this study, as well as a discussion of the significance of this study to the aerospace community of interest.

The second section of the study is a review of literature section which provides additional information on the NextGen air traffic control system and will be organized to examine the least significant to most significant articles in relation to NextGen Active Network and ADS-B design, features, operational concepts, information exchange requirements, and known security concerns. A summary of computer network security best practices including the most relevant aspects found pertaining to industry best practices and government standards of network security risks are included.

A discussion of methods used for this research comprises the third section of the study, and includes a description of the research design, a description of the sample selection process, the instrumentation used, and the data analysis methods used in the study.

The fourth section includes a description of each participant's background, organizational affiliations, professional and academic credentials to show the depth of knowledge within the selected sample. Findings from each of the participants interviewed are included which will be used to analyze the qualitative data collected. A summary of the findings is included.

The fifth and final section includes conclusions regarding the security objectives for the study and recommendations based on the literature and findings presented in this study, with additional recommendations for future research resulting from this study.

CHAPTER II

REVIEW OF LITERATURE

Introduction

In this section of the study, a review of related literature on the topics of the NextGen air traffic control system and industry best-practices for computer network security will be given. The purpose of the review is to orient the audience to network security risks in relation to the proposed NextGen Active Network. Multiple articles will be summarized in reverse order of relevance. Articles are broken into two primary categories:

- Studies and reports containing background information regarding the design of the NextGen air traffic management system, the associated active network(s) used for ADS-B, and available documentation discussing the potential security risks of NextGen system;
- Computer network security standards and best-practice documents against which to analyze the potential risk of the NextGen specifications.

Following the literature review is a summary of the most relevant information regarding the risk analysis.

Throughout the review of the literature, triangulation was used to assist in the development and confirmation of key concepts for the study, as shown in Figure 1.

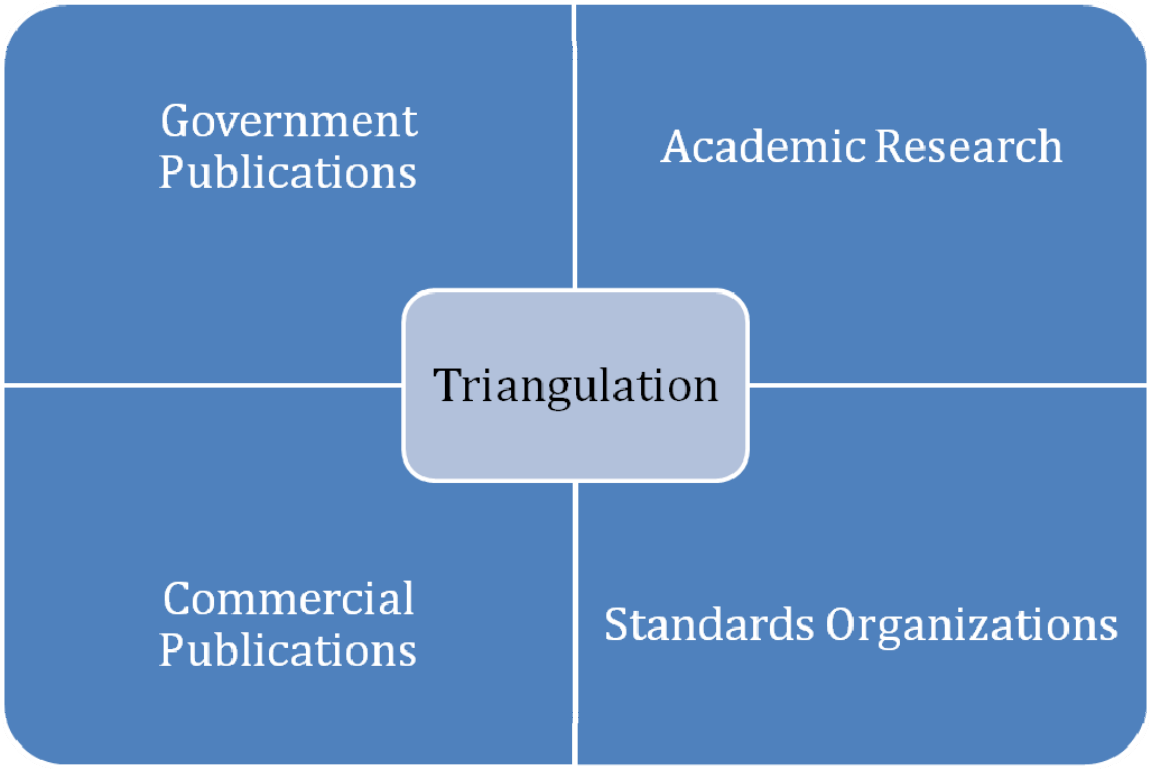


Figure 1. Triangulation Model.

NextGen Active Network: ADS-B

Several documents have initially been identified for inclusion in this study of NextGen. To understand the overall design of the NextGen system, the Concept of Operations for the Next Generation Air Transportation System which was developed by the Joint Program Development Office has been reviewed (JPDO, June, 2007). The Concept of Operations document specifies eight key capabilities necessary to achieve goals of NextGen, which include:

- Network-Enabled Information Access
- Performance-Based Operations and Services
- Weather Assimilated into Decision-Making

- Layered, Adaptive Security
- Broad-Area Precision Positioning, Navigation and Timing Services
- Aircraft Trajectory-Based Operations
- Equivalent Visual Operations
- Super-Density Arrival/Departure Operations

The benefits and incentives of moving to ADS-B are also highlighted in the initial ADS-B Aviation Rulemaking Committee report (ADS-B Aviation Rulemaking Committee, 2007).

NextGen Features and Concepts

The NextGen Concept of Operations document states that "at the heart of the NextGen concept is the information-sharing component known as net-centric infrastructure services or net-centricity" (Joint Program Development Office (U.S.), 2007b, p.ES-2) and that the net-centricity component binds NextGen operational and enterprise services together creating a cohesive link. The suite of enterprise services are to include "shared situational awareness, security, environment, and safety. (Joint Program Development Office (U.S.), 2007b, p.ES-2)"

There are significant differences between the ADS-B solution being fielded in Europe, China, and Australia versus the NextGen ADS-B solution which allows users to select from two different versions of the data link for use in the United States. International and U.S. solutions both utilize the 1090-ES data link which is already installed in some fashion on virtually all air carriers and many general aviation aircraft in the form of a Mode S or Mode AC transponder; however, the U.S. solution also includes

a second more robust data link using the UAT standard which has been proposed for use in general aviation aircraft operating below 24,000 feet. The UAT link provides additional bandwidth for uploading weather, radar, and additional in-flight data services which 1090-ES cannot accommodate. The dual data link solution requires ground-based transceivers in order for both types of aircraft to receive information from aircraft transmitting on the other data link.

A graphical overview of the NextGen system including the various communities of interest, federal agencies, industry and users as shown in the Concept of Operations is shown in Figure 1 (Joint Program Development Office (U.S.), June, 2007). The focus of this study is the ADS-B portion of the NextGen Active Network, particularly focusing on the security aspects of both UAT and 1090-ES data links between aircraft and ground-based transceivers which operate on both frequencies.

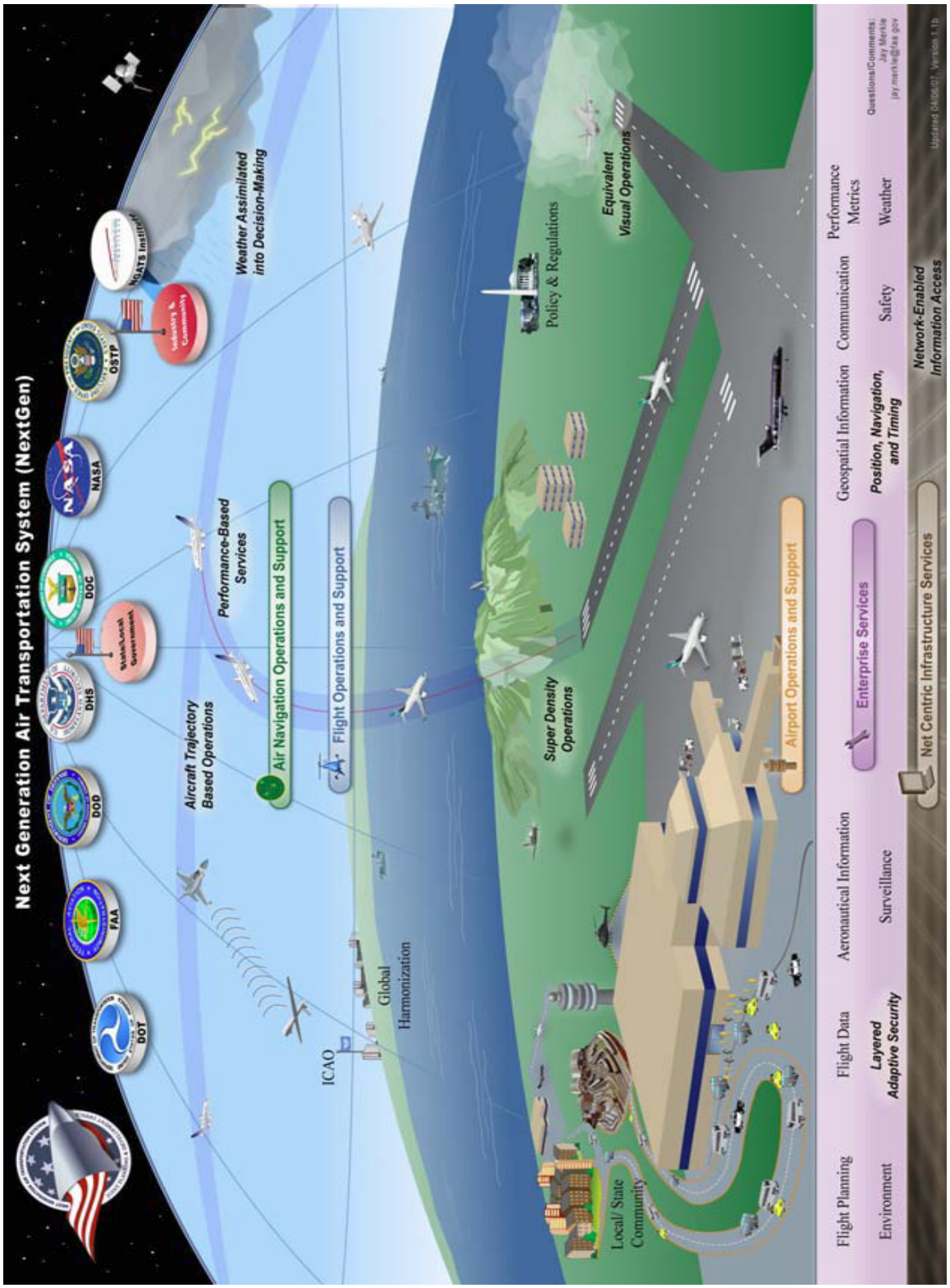


Figure 2. NextGen Functional Diagram. Note: From the Next Generation Air Transportation System Enterprise Architecture (Joint Program Development Office (U.S.), 2007a, p.23)

Two of the more notable differences between the existing radar-based air traffic management system and the proposed NextGen air traffic management system's ADS-B backbone revolve around the ability to not only provide high fidelity position information to air traffic controllers, but to also share that information between all NextGen equipped aircraft within both radar and non-radar service areas. Additional features of NextGen include the ability to display additional networked information including weather and traffic information without onboard radar or TCAS using the FIS-B and TIS-B services. A functional diagram of the ADS-B system is shown in Figure 2 (ADS-B Aviation Rulemaking Committee, 2008).

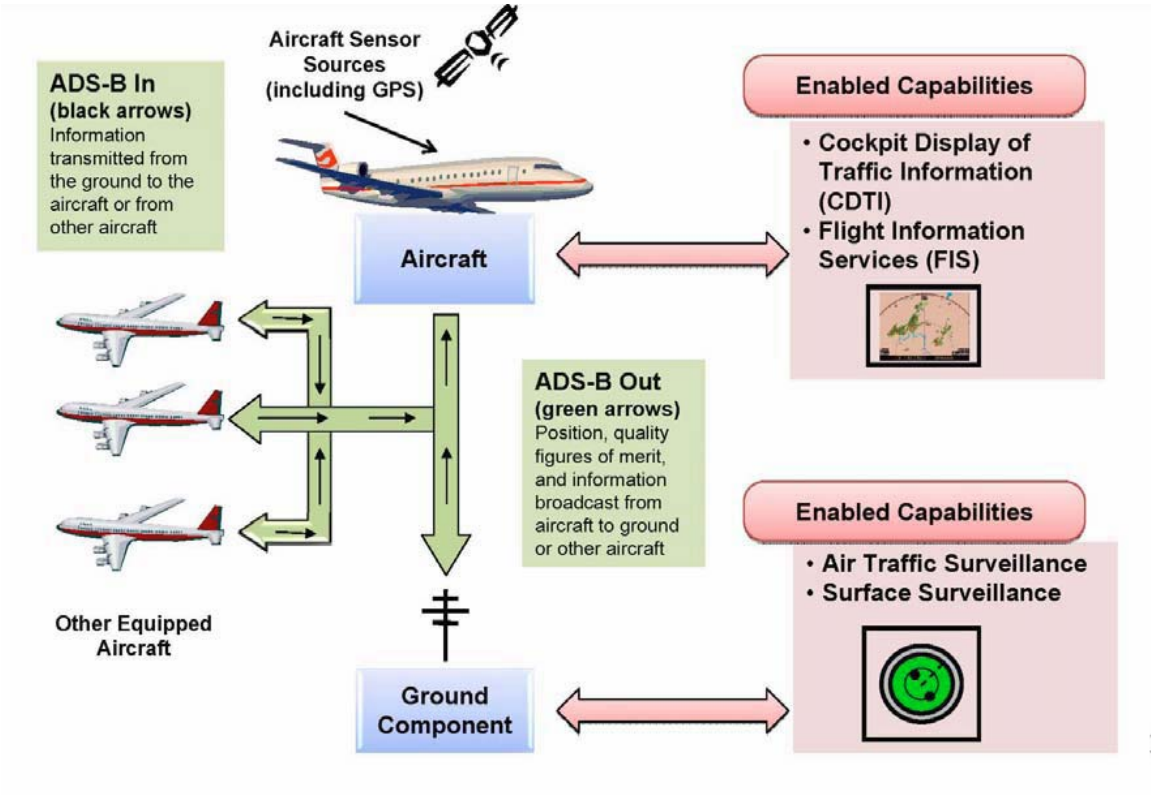


Figure 3. ADS-B Functional Diagram (ADS-B Aviation Rulemaking Committee, 2008, p.D-3).

A sample CDTI display is shown in Figure 3 including a ground-based weather radar overlay transmitted via the NextGen Active Network integrated into the pilot's display. In the initial implementation of NextGen, this information is limited to aircraft utilizing the UAT link and within 200 nautical miles of a ground based transceiver (ADS-B Aviation Rulemaking Committee, 2008).

Figure 4. Sample CDTI Display including Weather. (ADS-B Aviation Rulemaking Committee, 2008, p.D-7)

Traffic information combined from both ADS-B signals and ground-based secondary surveillance radar may also be received via ground based transceivers of the NextGen system, and is also limited to the UAT link. A sample ADS-B display showing integrated traffic data is shown in Figure 4 (Flt Tech Online, 2009).

Figure 5. Sample Garmin ADS-B cockpit display including traffic and weather (Flt Tech Online, 2009).

Another important feature of NextGen is improved management of aircraft and vehicular traffic while on the ground at airports. The NextGen system is designed to assist in preventing accidents by displaying all ADS-B equipped vehicles on the CDTI. This could include not only aircraft taxiing, taking off, and landing but could also encompass other service vehicles at airports including fuel, catering, freight, and other maintenance traffic common to airport operations. A satellite view of the Louisville International Airport including an inset of the cockpit version of the ground airport display is shown in Figure 5. This feature is particularly useful for night or foul weather operations(ADS-B Aviation Rulemaking Committee, 2007).

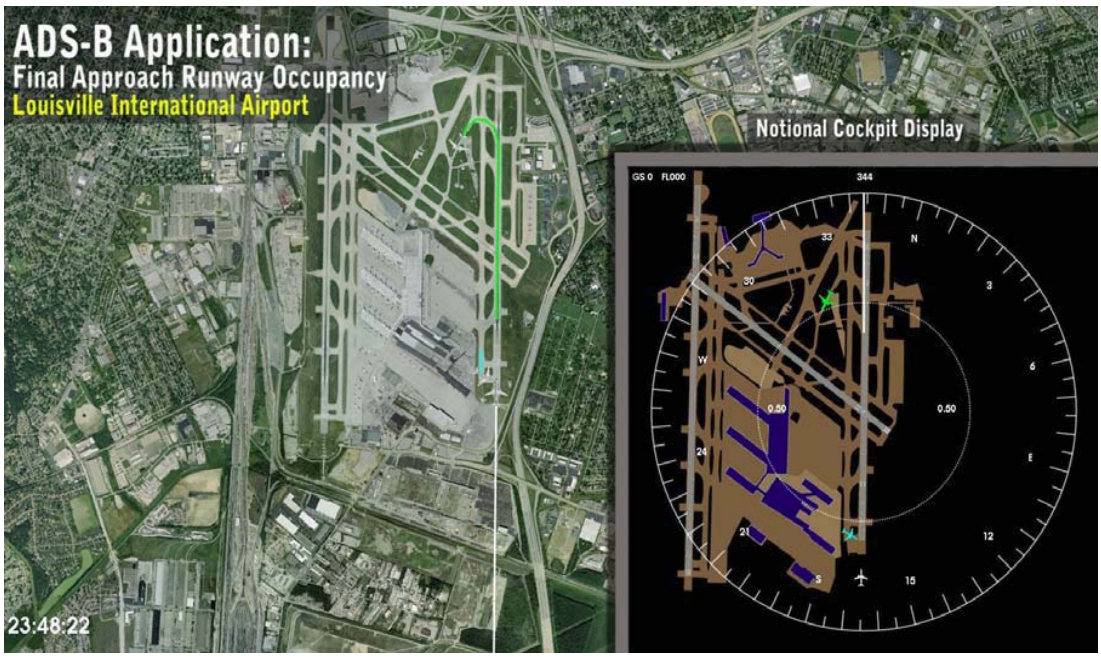


*Figure 6.*Sample ADS-B ground traffic display (ADS-B Aviation Rulemaking Committee, 2007, p.25)

Applying the advantages provided by NextGen through the use of ADS-B and associated technologies will allow reduced separation of aircraft flying into and out of high density airports such as Atlanta, Chicago, and Los Angeles which are currently limited by the accuracy and timeliness of radar information. Reduced separation increases the usability of the ground facility by increasing the number of aircraft that may takeoff and land within a given timeframe negating the need for additional runways and flight delays. Oceanic and other remote areas not covered by existing primary radar services also benefit from these services as current in-trail standards require a 15 minute window separating aircraft flying between continents. The bottom line to all of the advances and advantages within ADS-B and the NextGen air traffic control system is increased safety and efficiency within the national airspace system.

Safety and efficacy testing of the ADS-B concept was accomplished in the Alaskan region by the FAA beginning in 1999 through no-cost equipage of all FAA Part 135 aircraft. The increases in safety during the test have been quantitatively shown in other studies, including a Northcentral University study which concluded that ADS-B technology "had an effect upon the reduction of the accident/incident rates in the Alaskan region" (Gardner, 2005, p.115). ADS-B has already been fielded in Australia, Canada, China, and multiple standards organizations have moved to standardize on the 1090-ES platform of ADS-B including ICAO and Eurocontrol. Though very similar in practice, ADS-B systems are not entirely standardized. An assessment of the similarities and differences between NextGen and SESAR, the system being fielded by Eurocontrol, was reviewed for security ramifications (Joint Program Development Office (U.S.), 2008a).

NextGen Network

To better understand the specifics regarding the information exchange requirements with the NextGen Active Network, a thorough review of Next Generation Air Transportation System (NextGen) Enterprise Architecture (JPDO, 2007a) was undertaken. Appendix E: OV-3 is the portion of the Enterprise Architecture document containing the most comprehensive description of operational information flow and is designed to facilitate *information-centric* analysis. For each of the seventeen information exchange requirements described in the document, specific attributes including name, description, source activity, operational node and sub-node, destination node and sub-node, and destination activity were outlined. Of particular interest to this study was the statement that additional attributes to the information exchange requirements could include such details information assurance, confidentiality, availability, integrity, access

control, and dissemination control, which directly correlate with existing information security standards. The current version of the NextGen Enterprise Architecture does not include these details (Joint Program Development Office (U.S.), 2007a).

As the NextGen program is still under development, the Joint Program Development Office does make a *maturity statement* that OV-3 will continue to grow in detail and maturity as the Enterprise Architecture is reviewed by stakeholder and working groups. In conjunction with the Enterprise Architecture document, a review of the Security Annex Concept of Operations v.2 for the Next Generation Air Transportation System (JPDO, 2007b) was also conducted. Again, as the NextGen system is still under development, there are thoughtful descriptions of the overall concepts intended to provide integrated risk management by insuring secure people, secure airports, secure checked baggage, secure cargo and mail, secure airspace, and secure aircraft, but specifics regarding communications methodology are limited to pointers toward the 1090-ES and UAT standards which have been developed through RTCA, Inc., a consortium of interested government and industry representatives.

Other literature reviewed to gain perspective on the technologies in use within the ADS-B portions of the NextGen network, relative assessment of their security as a medium for air traffic control, and discussion of security needs within airborne networks included a study conducted at MIT which states that ADS-B broadcast data is not secure (Jochum, 2001) . A conference paper presented at the Digital Avionics Systems Conference regarding efficient data link security states “Much like the Internet, this aeronautical communication environment is vulnerable to attacks by external entities , which may accidentally or maliciously jeopardize the safety and integrity of the ATN.”

(Olive, 2001, p.9.E.2-2); and went on to mention that "The primary areas of vulnerability are the air-ground data link and the terrestrial networks, which may include both private and public communication networks (Olive, 2001, p.9.E.2-2)." Olive specifically discusses the needs for message authentication, data integrity, and access control although data confidentiality or encryption was excluded as it is "not an ICAO specified security requirement" since "communication monitoring and message traffic analysis do not pose a threat to air traffic safety (Olive, 2001, p.9.E.2-3)".

To zero in on the specific capabilities and limitations included in the current design of the NextGen Active Network, design documents describing communications methodologies from the Minimum Operational Performance Standards for both 1090-ES and Universal Access Transceiver Automatic Dependent Surveillance-Broadcast documents were reviewed. The 1090-ES standards have been developed over a number of years and have been designed around legacy support for existing radar transponder technologies (RTCA Inc. (Firm), 2006). The UAT standards have been developed much more recently and include additional capabilities such as larger packet sizes, higher transmission speeds, anonymous mode and encryption (RTCA Inc. (Firm), 2002). Another recent perspective which includes a discussion of ADS-B communications in the context of net-centric systems and applications or *eEnabled aircraft* is discussed and expresses concerns that "off-the-shelf wireless solutions can open vulnerabilities that give rise to security concerns with the eEnabled airplane (Sampigethaya, Poovendran, & Bushnell, 2008, p.1)."

Known Concerns with ADS-B Security

The Federal Aviation Administration process for developing the new regulations which will define and mandate the phase-in and usage of ADS-B over the next 16 years involves a Notice of Proposed Rulemaking, establishment of an Aviation Rulemaking Committee which includes government and interested parties, and discussions between the industry, public, and the FAA prior to dissemination of final regulations. As of this writing, the ADS-B Aviation Rulemaking committee has published two papers highlighting the benefits of ADS-B (ADS-B Aviation Rulemaking Committee, 2007), and more recently a set of recommendations regarding the use of ADS-B within NextGen.

Several of the latest recommendations from the ARC focus on security considerations. Comments to the ARC on FAA Notice of Proposed Rulemaking 7-15 show that "17 commenters, including 2 domestic air carriers, an avionics manufacturer, an association, and the DOD commented that the ADS-B system was vulnerable to being used for malicious purposes.(ADS-B Aviation Rulemaking Committee, 2008, p.96)" The malicious purposes mentioned include contentions that both 1090-ES and UAT are susceptible to denial jamming in the vicinity of ground stations, that 1090-ES is vulnerable to deceptive jamming (though UAT is less so), and that the proposed design is susceptible to the transmission of phantom aircraft identities, locations and velocities. The ARC responds that "there is no greater threat to ADS-B aircraft than those with transponders or ACAS." (ADS-B Aviation Rulemaking Committee, 2008, p.99). The rulemaking committee agrees that ADS-B spoofing is possible, but believes that alternative surveillance systems such as SSR, the use of passive multilateration, and non-

cooperative surveillance systems are adequate to validate ADS-B reports and prevent spoofing. The ARC recommends that FAA and other appropriate government agencies continue to study means of mitigating loss of GNSS signals due to intentional or unintentional interference. Although the FAA's current implementation plans call for retention of SSR and elimination of primary radar, NextGen budget proposals show a $287 million annual cost savings by elimination of radar.

The most recent version of the NextGen Integrated Work Plan, released in September of 2008, highlighted the many moving parts that must be integrated to successfully implement the NextGen air traffic control system. One of the appendices included in the IWP discusses outstanding policy issues which must be addressed prior to successful implementation (Joint Program Development Office (U.S.), 2008b). Three policy issues were of interest to this study:

- PI-0017, which calls for a policy to define the strategy for communications services in ground, space, airborne, and/or performance-based architectures and include a decision on use of an *airborne internet*.
- PI-0021, which calls for a policy to protect access to over-the-air ADS-B and data communications information to prevent unauthorized use of information. This issue goes on to state that the current "policy must change or ADS-B standards and avionics must be modified to transmit encrypted information. (Joint Program Development Office (U.S.), 2008b, p.Appendix IV-5)"
- PI-0024, which calls for the development of policies to define the organization(s) that will maintain ownership of a central information repository, handle archived data to protective privacy and proprietary

information, and act as a liaison with ICAO. This issue goes on to recommend that the NextGen unclassified Mobile Routing and Domain Network Services operated by the FAA be utilized as the root of the domain for establishing policies and protecting information.

Another recent study, co-presented by representatives from France and Australia at the Seventh Meeting of ADS-B Study and Implementation Task Force sponsored by ICAO in Chengdu, China during August of 2008 squarely addressed the three pillars of network security described in the Federal Information Security Management Act citing considerations toward data confidentiality, integrity, and availability (ICAO, 2008). The study includes recommendations that the aviation community should be "aware of possible ADS-B security specific issues (ICAO, 2008, p.5)" and should "address appropriate mitigation applicable in each operational environment, in accordance with ATM interoperability requirements. (ICAO, 2008, p.5)" The final recommendation of the study suggests that "additional studies should be made to identify potential encryption and authentication techniques" but also that the "distribution of encryption keys to a large number of ADS-B receivers is likely to be problematic.(ICAO, 2008, p.5)"

Computer Network Security Best-Practices

To develop a baseline for IT industry best practices, several government and commercial sources were selected. Two companies in the United States represent the majority of computer network operating systems and network routing and switching: Microsoft and Cisco Systems. Due to their market standing, both companies invest heavily in security research, and assist their user communities in expanding the body of knowledge regarding security best practices. In addition, the National Institute of

Standards and Technology represents a compendium of thought leadership within the computing and network environments.

Cisco Systems Changed Threat Landscape

Cisco Systems is the world's largest manufacturer of routing and switching equipment currently holding a 51% share of the service provider router market. As a leader in the network industry, Cisco continuously researches security issues and publishes white papers regarding identification and mitigation of network security threats which give a broad view of the risks to computer networks. The threats experienced by contemporary computer networks are far removed from those envisioned when the Internet was conceived. The differences in security requirements are referred to as the Changed Threat Landscape, and graphically depicted over time in Figure 6 (Cisco, 2007).

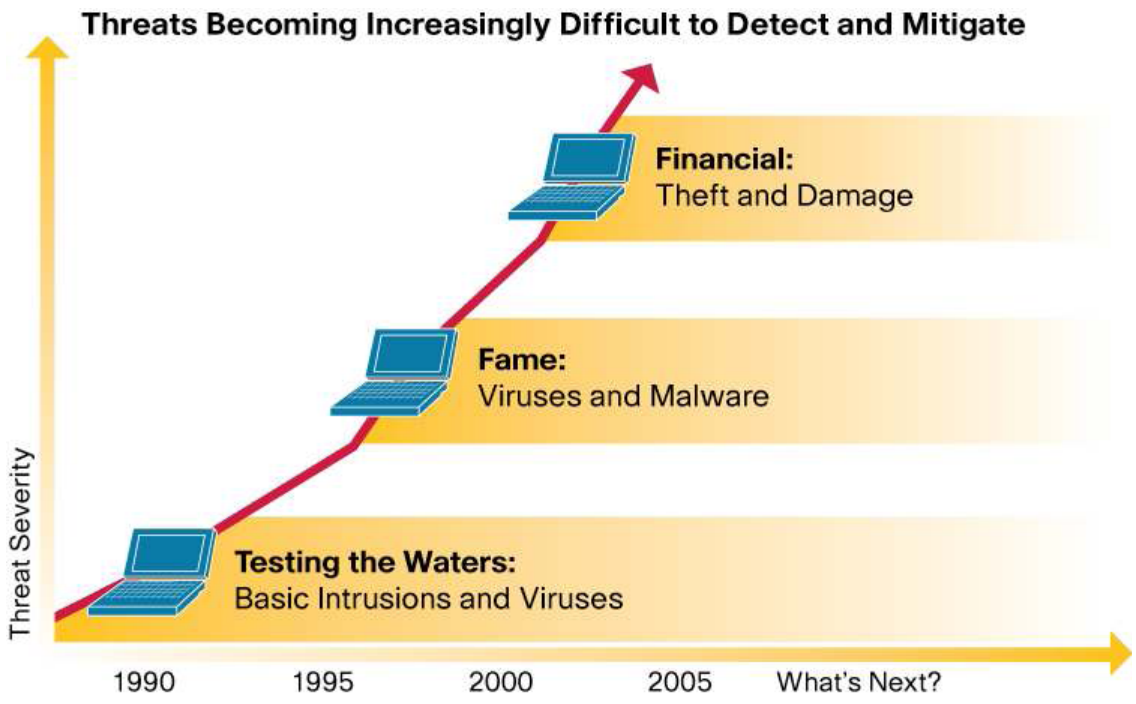


Figure 7. The Changed Threat Landscape, (Cisco, 2007, p.1).

Microsoft Security Development Lifecycle

Microsoft also has a large interest in systems and network security with over 89.6% of the operating system market worldwide. Microsoft has taken an aggressive stance toward security following several large-scale security breaches and as early as 2002 enhanced security through their Trustworthy Computing initiative. Microsoft's latest network operating systems and applications are developed using common standards and industry best practices based on the Security Development Lifecycle (SDL) and toolsets which include the SDL Threat Modeling Tool and Optimization Model which are freely shared with the public (Keizer, 2008). Microsoft's methodologies for defining and containing risks give a different perspective from Cisco, and yet focus on current and coming threats in securing data networks. The framework for the Security Development Lifecycle is shown in Figure 7 (Microsoft, 2009). The current state of the NextGen air traffic control system falls between the Requirements, Design, and Implementation phases of the Security Development Lifecycle as described in Version 2.0 of the NextGen Enterprise Architecture (Joint Program Development Office (U.S.), 2007a).

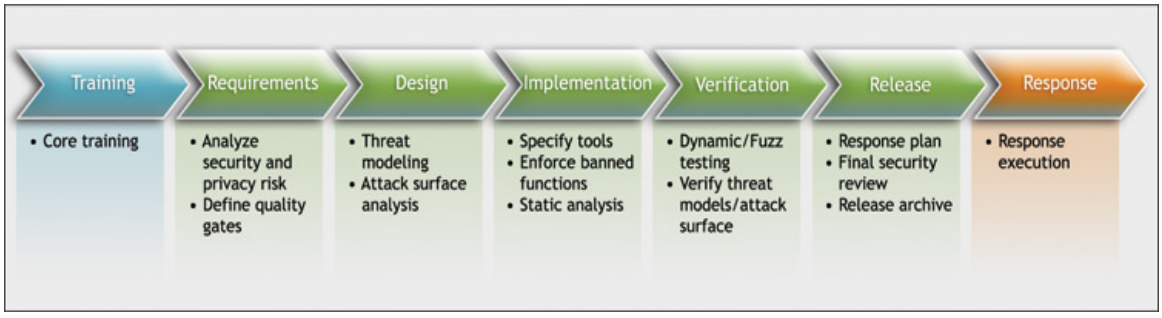


Figure 8. The Microsoft Security Development Lifecycle, (Microsoft, 2009, p.1).

Government Standards and Industry Best Practices

The security studies and publications presented in the commercial sector translate to, and are often the result of, academic studies and government standards developed within the public sector. A series of documents were reviewed for applicability to this study, primarily utilizing the document library of the National Institute of Standards and Technology.

Within the past six years, NIST has published a series of special publications which were also used as reference points while developing the research questions and interview questionnaires for this study, including the Risk Management Guide for Information Technology Systems (National Institute of Standards and Technology (U.S.), 2002a), Wireless Network Security (National Institute of Standards and Technology (U.S.), 2002b), Guideline on Network Security Testing (National Institute of Standards and Technology (U.S.), 2003), Recommended Security Controls for Federal Information Processing Systems (National Institute of Standards and Technology (U.S.), 2006), and Guide for Mapping Types of Information and Information Systems to Security Categories (National Institute of Standards and Technology (U.S.), 2008).

The review of NIST special publications' applicability to NextGen airborne network issues highlighted two standards from the Federal Information Processing Standards library. FIPS Publication 191 which provides guidance for the analysis of local area network security was reviewed, however, it was deemed a poor fit in that the NextGen ADS-B airborne network differs significantly from a conventional LAN. ADS-B aircraft and ground transmissions are intended to be received by all aircraft and ground stations within a reception radius and therefore the scope of the network cannot be

defined “within a moderately sized geographic area over a physical communications channel of moderate rates” (National Institute of Standards and Technology (U.S.), 1994, p.6). FIPS Publication 199 was also reviewed to categorize the security risks inherent to the NextGen ADS-B network. Table 3 summarizes the potential impact definitions for each security objective of confidentiality, integrity, and availability (National Institute of Standards and Technology (U.S.), 2004).

Table 3.

Potential Security Impact Definitions, adapted from FIPS Pub 199 (National Institute of Standards and Technology (U.S.), 2004)

	POTENTIAL SECURITY IMPACT		
OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorized disclosure of information could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity	The unauthorized modification or destruction of information could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals
Availability Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals

FIPS Publication 199 defines that security categorization, or SC, can be expressed as a generalized format using: SC information type = [(confidentiality, *impact*), (integrity, *impact*), (availability, *impact*)] where the acceptable values for each potential impact are low, moderate, high, or not applicable. The airborne and ground-based ADS-B links used by the NextGen air traffic control system would therefore be classified as shows in Table 4.

Table 4.

NextGen ADS-B Security Categorization

Security Objective	NextGen ADS-B Categorization
Confidentiality	***Low.*** ADS-B information is transmitted *in the clear* to allow other aircraft to recognize and respond to potential conflicts. There is a potential that tracking information captured by unauthorized sources could use the data for commercial gain (privacy issue). This would not cause a NextGen system disruption.
Integrity	***High.*** If ADS-B data is improperly modified, destroyed, or false information is transmitted from a non-authentic source the NextGen air traffic control system could become unusable and legacy air traffic control methods would have to be employed to prevent a complete loss of system usability.
Availability	***High.*** If the 1090-ES and/or UAT links used to support ADS-B data experience interference due to jamming, denial of service, or excessive data traffic the NextGen air traffic control system could become unusable and legacy air traffic control methods would have to be employed to prevent a complete loss of system usability.

The Security Categorization formula for the NextGen ADS-B network can be expressed as: SC = (Low, High, High), or averaged across all three objectives as: SC = High.

Summary of the Literature Review

The NextGen air traffic control system is poised to provide dramatic improvements to the management of air travel, in-flight safety, and airport scalability worldwide. Although the NextGen enterprise architecture and security annex specifications indicate that secure network communications are to be included in the system design, other available literature indicates that network security has been considered but is not a demonstrated part of the existing design when compared to industry best practices including both government and commercial standards.

CHAPTER III

METHODOLOGY

Introduction

In the Methodology section of the study, three primary topics are discussed. The first topic covers the research design including the qualitative risk analysis. The second topic includes the selection of the sample. The third topic of this section presents the type of instruments that were used to collect data for this study and their reliability and validity, the overall design of the study, and its' appropriateness in answering the proposed research questions. A final description of the procedure used to conduct the study is also included.

Research Design

Qualitative Risk Analysis

The research design selected for this study is a Qualitative Risk Analysis. Qualitative Risk Analysis assesses the impact and likelihood of the identified risks in a rapid and cost-effective manner. By evaluating the priority of risks with consideration to impact on NextGen's security objectives, this design provides a foundation for additional focused quantitative analysis or follow-on risk response plans.

Selection of the Sample

This study utilized a combination of purposive and qualitative sampling leading to a snowball sampling technique. Purposive sampling is typical of qualitative research. The initial purposive sample of organizations was selected because the organizations were engaged in the design, development, implementation or user community surrounding NextGen and were "believed to be representative of a given population" (Gay, et al., 2006, p. 113). Because the study was qualitative in nature, initial individuals from the sample organizations were selected using qualitative sampling based on their ability to become "key informants" (Gay, et al., 2006, p. 113). From the initial qualitative sample of individuals, a snowball sampling technique was employed to discover additional perspectives for the study.

The initial government and industry institutions selected for this study include the Federal Aviation Administration (http://www.faa.gov) as the regulatory branch of the government handling aviation, the Joint Planning and Development Office (http://www.jpdo.gov) which is responsible for the development of the standards used for the NextGen air traffic control system, the Department of Defense (http://www.dod.mil) which is one of several federal agencies actively participating with the JPDO in NextGen development, the Department of Transportation (http://www.dot.gov) which provides research to the FAA regarding NextGen technologies, the Aircraft Owners and Pilots Association (http://www.aopa.org) which represents the interests of thousands of both pilots and aircraft owners, and L-3 Communications (http://www.L-3com.com) which

has multiple divisions providing advanced NextGen compatible avionics and systems to both general and commercial aviation.

The selection of this purposive sample is important because each selected organization had a different perspective on the issues representing implementation, regulation, design, manufacturing, pilots, and owners; and each group had its own resources to interpret the proposed standards for the NextGen Active Network. Although the organizations were geographically disparate, their perspectives were all important. From the initial organizations selected, a snowball sampling technique was used to determine other specific individuals and/or additional organizations with information pertinent to this study. The sample size for the study was determined by the number of participants whose organizations would formally approve participation. Although six formal interviews were successfully completed for this study, several additional interested resources were located within organizations but were unable to obtain the required organization approvals and could therefore not participate in the study.

Accessibility was a secondary consideration given to these selections in conducting the study. The researcher has existing relationships with members of several organizations and made contact with the correct management personnel to insure feasibility. The researcher had access to engineering and technical personnel in offices pertinent to this study, and was allowed access to any other person or office that the researcher determined to be a viable contributor within the organizations.

The sample size for the study was determined by identifying "participants who meet the defined criterion" and selecting "a group of five or so participants to collect data from" (Gay, et al., 2006, p.115). The determination to utilize five or more participants

was retained as a minimum and additional participants were identified and recruited until this criteria was exceeded.

The selection of participants was critical to the success of this study. The quality of interview based research is directly related to the expertise of the participants. For this study, experts were selected based on their experience, education, and technical expertise within the aviation data communications realm. Several of the members qualified in multiple areas with experience in air traffic control, aviation communications, and computer science. Table 5 illustrates the diversity of the study sample. Please note that the participant numbers have been removed and information presented in random order to insure the anonymity of the participants.

Table 5.

Participants by Discipline and Market Segment

Discipline				Market Segment
Aviation	**Avionics ADS-B**	**Academia**	**Computer Science**	
■	■	■	■	Commercial
■				Government
■	■		■	Commercial
■	■			Commercial
■	■			Commercial
■	■		■	Government

Instrumentation and Procedures

The instruments used in this study were questionnaires or interview guide. The rationale behind selecting these instruments was the depth of data, the ability to ask questions that could not be effectively structured into a multiple-choice format, the flexibility of interaction, the likelihood of more accurate and honest responses, and the ability to follow up on questions that one-on-one interviews produce (Gay, et al., 2006, p. 173). A standardized questionnaire was developed (see Appendix C) and used to conduct all interviews included in the study. The questionnaire was piloted by both academic and industry personnel prior to initial interviews.

Interviews were conducted with key people at each institution to solicit overall answers to the research questions. To enhance validity and reduce bias within the interviews, a series of consistent steps were followed. The steps used for each interview are shown in Table 6. The purpose of conducting these interviews was to extract the richest possible information from sources with pertinent understanding of the airborne and ground-based network links utilized for ADS-B transmissions within the proposed NextGen air traffic control system. The selection of a purposive sample requires that "qualitative researchers who use these techniques must provide detailed information about research participants and how they were chosen (Gay, et al., 2006, p.114)

Table 6.

Interview Procedures

Step	Procedure
Introduction	The topic of the study and researcher was introduced to each participant. The Interview Question Guide was made available for review by the participant and/or organization.
Research Approval Documentation	Executed Organization Approval letter and Informed Consent Form are collected from the participant.
Interview Setup	Specific times and locations were selected for the interview to minimize interruptions and background noise. Fresh batteries were installed in the digital voice recorder, and the recorder was checked to insure that adequate free space for the complete interview was available.
Interview	The interview consisted of asking each of the 18 questions within Section A and Section B of the Interview Question Guide, in sequence, to each participant. Participants were allowed to take whatever time they felt necessary to answer each question completely, and when appropriate, follow-up questions were asked to clarify their response. Acronyms and technical terms used by the participants were confirmed to avoid misunderstanding. Written notes were also taken by the researcher to highlight key responses and allow for follow-up questions or external confirmation through literature review. A bio was obtained from each participant.
Post Interview	Immediately following the interview, Section C was completed by the researcher to insure that the digital recordings could be correlated to biographical information from each participant for internal use. The recording was then transferred to a secure server where it was later accessed to transcribe the interview into a Microsoft Word document.

The study was designed to insure the trustworthiness of answers by conducting interviews over several months to compare differing responses. Digital recordings and

field notes were used during each interview. Triangulation was used to supplement interviews by reviewing available documents from each organization.

Data Analysis

The data collected for this study consisted of multiple elements including each participant's education and career background, organizational affiliation, current position held, and availability. Each interview was recorded using a digital audio recording device, which was then transferred to a secure server for storage, transcription, and analysis. The recordings were transcribed into their literal written form using Microsoft Word. Notes and observations were also stored from each interview and utilized as additional data. Transcribed data were then coded, compared, and synthesized for placement into categories in order to answer the research questions designed for the study.

In addition to manual coding and analysis, both audio and transcribed interview data, internal and external literature resources, scanned images and graphics were loaded into NVivo version 8 software for secondary analysis and confirmation of manual results. While NVivo has powerful capabilities, it requires a significant amount of training to be most effective. The E-project developed by this study using NVivo was not fully exploited due to the researcher's limited experience with the product and the overall timeframe allotted for NVivo training and use. Subsequent qualitative studies by the researcher will more effectively be able to utilize the software to produce additional reports and diagrams not included in this study.

CHAPTER IV

FINDINGS

Introduction

The findings for this study have been developed from over a hundred pages of interview transcripts taken from six NextGen stakeholders who ranged from government program managers to avionics engineers, computer scientists, and aviation consultants. The study was designed to identify and understand the risks inherent to the proposed implementation of the active network within the ADS-B portion of the NextGen air traffic control system and compare the enterprise architecture against current standards and best practices in computer network security. Each stakeholder brought his or her own unique perspective to the problem at hand as it applies to aviation, avionics, and network security.

A comparative risk analysis against existing security standards was performed. The cross-pollination of information between multiple perspectives, as demonstrated in Table 5 and Table 7, provided a unique depth and enhanced the inductive nature of qualitative research (Gay, et al., 2006, p. 402).

Sample Depth of Knowledge

To balance the need for richness of information against the requirements to maintain participants' anonymity, the background of the participants was presented in a manner to avoid correlation with questionnaire responses. The order of presentation for background information and questionnaire responses has been purposely altered to further mask the individual's characteristics. Table 7 summarizes the depth of knowledge of the participants for this study.

Table 7.

Depth of Knowledge of Participants

Areas of Expertise	Background
Aviation, Avionics, Computer Science, Consulting, Academia	This participant has worked as a technical consultant for over 10 years, holds Master's and Doctoral degrees in Computer Science from Oxford, is a Rhodes scholar, and a founding participant in two groups which have been awarded the Collier Trophy. The participant is a subject matter expert in ADS-B and currently a member of IEEE, RTCA, and ICAO ADS-B industry standards committees. Prior positions span nearly 30 years and include research manager, project manager, vice-president, president, and assistant professor.
Aviation, Operations, Systems Management, Defense, Space Operations, Security	The participant was a high ranking military officer who holds a Bachelor's degree from the Air Force Academy, a Master's in Systems Management, has served in several capacities for Space Command, the Pentagon, the U.S. Senate, and is currently a director with oversight responsibilities for net-centric operations at a federal agency.

Areas of Expertise	Background
Aviation, Avionics, Computer Science	The participant has worked as an engineer for multiple commercial organizations in aviation, avionics, and remotely piloted vehicles for over 25 years. The participant holds Bachelor's degrees in Electrical Engineering and Computer Science, and holds multiple patents surrounding TCAS, Mode S, ADS-B, RF, and surveillance technologies. The participant is currently a senior staff engineer for a commercial avionics manufacturer.
Aviation, Avionics, Rulemaking	The participant holds Bachelor's and Master's degrees in Engineering, has over 25 years of experience in the aviation industry, and is considered an expert in surveillance systems (ADS-B, TCAS, TAWS), data communication systems (ACARS, CMU), and flight management systems. The participant is currently a member of multiple ADS-B industry standards groups and the ADS-B Aviation Rulemaking Committee. The participant is presently technical senior staff for a commercial avionics manufacturer.
Aviation, Avionics	The participant holds a Bachelor's degree in Electrical Engineering and has worked in avionics development for multiple commercial entities for over 28 years in the development of RF systems including TCAS, transponder, VOR and ADF. The participant is also an FAA System and Equipment DER, and is currently a senior engineer at an avionics company providing equipment for the initial rollout of ADS-B in the air freight industry.
Aviation, Security, Information Systems, Project Management	The participant is a noted information security specialist who holds a Bachelor's degree in Electrical Engineering and has over 25 years of progressive security design and implementation experience including designs for Olympic venues, the Air Force, the State Department, the HSPD-12 initiative, and other large-scale security implementations. The participant has been employed in both commercial and federal market segments, but currently acts as a division chief and subject matter expert over infrastructure protection for a federal research facility providing thought leadership to multiple federal agencies.

Confidentiality

Participant #1

Based on background and experience, Participant #1 indicated that there are published standards for ADS-B communications between aircraft and between aircraft and the ground so that anyone with an appropriate receiver and a standard decoder can listen in and figure out precisely what the aircraft are transmitting. The participant synopsized his or her perspective of confidentiality within NextGen ADS-B transmissions by stating "For that part of the network, absolutely no security." Participant #1 went on to elaborate that the rationale behind the lack of confidentiality "is by design intended to be heard by receivers because there is not only the air to ground aspect for classical ATC control, but there is also the air to air applications from pure situational awareness and eventually spacing and delegated separation."

In order for NextGen to perform its' intended mission of providing air traffic control, every aircraft must be able to receive information from other aircraft in their vicinity whether directly or via a ground based transceiver. The participant highlighted this need by stating "In our air space, particularly in our highest density air space, it must not be a secret that an aircraft is close to you", and continued that "it absolutely should not be a secret that I am converging on you two miles away on a collision course." The participant completed the discussion of confidentiality with an outline of existing regulations which have been in place for over 30 years for all aircraft flying within civil airspace which must, by rule, be equipped with a transponder that can respond to TCAS security issues.

The participant highlighted the differences between confidentiality and anonymity within the NextGen ADS-B transmissions by adding that the UAT link currently provides for an anonymous mode of operation similar to squawking 1200 on a legacy transponder by saying

> …there is great disagreement, differing views around the world as to whether the anonymous address should be usable; and a number of ICAO contracting states would never permit it to be used period. They understand that the United States has a situation in which they have 200,000 general aviation aircraft and, perhaps, a different political situation with regard to the way that the privacy laws are and that the airspace is regulated – but they do not want that anonymous feature used in their airspace.

The participant later returned to the confidentiality aspect of the study and reiterated their perspective by stating

> I think I have articulated that the air ground segment should not be changed, and I have given a number of reasons that it should not from a security perspective. It is a broadcast system. It is intended to be in the clear just like the GPS signals are. We should no more encrypt or provide other shielding mechanisms for broadcasts out of aircraft than we should reinstate selective availability on GPS that is off by presidential policy directive and has been since August of 2000. So we have moved past the argument with regard to GPS, and we should not create an argument that we will later need to move past for ADS-B aircraft transmissions.

Participant #2

Participant #2 indicated that "the envisioned net enabled operations architecture has not yet been instantiated." The participant continued to elaborate that "A major design element is enterprise level, multi-layered security that governs information exchange, thus preventing unauthorized disclosure." When discussing limits to confidentiality within NextGen, Participant #2 believed that the NextGen net enabled operations architecture envisioned "right data, right user, right time", and that data will be protected to the appropriate degree, as determined by the subject matter experts operating under the auspices of a Community of Interest.

Although this participant's comments speak to the future potential of the NextGen networks, the comments also highlight the possibility of initially fielding hardware and software solutions that may be forced to change as security issues are identified in implementation. This common concern was also expressed by several other participants in the study.

Participant #3

Participant #3 confirmed that confidentiality is not currently designed into the NextGen network, stating that "ADS-B information is sent on a particular RF channel per industry standards, with a particular modulation and there is no encryption." The participant spoke to the relative complexity of the receiving the ADS-B messages stating

> "someone would have to know how to build the correct equipment and then receive it and decode the address. The address field is a parity field, so you would have to decode that to find out if you wanted to know, like a particular mode S address for a particular airplane – and then you could get the data. I mean, but

you would have to go to some means, some technical means, in order to be able to receive and get the data. You know, if they are independent of the avionics industry that is using the equipment.

The bottom line to this participant's perspective on confidentiality within ADS-B was summed up in stating "The other airplanes need the information, right? That is to prevent collisions – that is the whole point."

Participant #4

Participant #4 outlined the confidentiality components within the NextGen Active Network by commenting that

> The airborne, the air to ground segment, of course, is not – does not provide any kind of security; but when you get down to the ground infrastructure, they have all kinds of security measures they put into place when they are passing this information over a network" and continued that ADS-B messages are "not any communications between individuals that would require some kind of secure communications that you are trying to keep information from getting into the wrong hands.

The participant compared the proposed NextGen system with the security risks of existing technology in stating that

> When you look it from what exactly you are trying to do here, you are basically trying to control aircraft in a controlled environment; and today you use radar and there is not a lot of security that is up on radar – you are just painting an aircraft or you are receiving information that is coming from the same source that is going to provide you the ADS-B data, so it is all positional and you are just receiving it.

> Now if you get into the automation and you start monkeying with the automation of what air traffic control is using, then yeah, I could see where there could be an issue there—but you certainly can receive the information and listen to it all day long (if you would like). They do that with ACARS today.

This participant did not view the public nature of the current NextGen data as a threat, unless "if there is a specific aircraft they are trying to find, then there might be an issue there."

Participant #5

Participant #5 indicated that proposed model for the NextGen network does not require confidentiality by stating that the network uses

> …public standards, and anybody can listen. There is no encryption or anything like that. Now there is a military format, which nobody is using to my knowledge that does have encryption. Military ADS-B – it is called the F19; but it, to my knowledge, it is not being used.

The participant continued, stating that "I mean – you have the terrorist aspect, which obviously is a problem. I suppose somebody could do bad stuff if they were intelligent enough to, but I do not… I have not thought about specific threats or anything like that."

The participant also indicated that the current reasons to broadcast information in the clear because "ADS-B has to be, I mean the airplanes, the air vehicles and ground stations both have to receive the data. If you could encrypt so, you know, the desired users can use it but other people could not, that would probably be good to do, but that is how it is set up today."

Participant #6

Participant #6 indicated that

> In the air, it is broadcast in the clear. It is basically because the current system is the same way – everything is in the clear. So if you have your own equipment and know how to interpret it, you can understand what is going on. And because it is a worldwide system, that they need to keep it in the clear. To get everyone on the same page is extremely difficult if you go encryption or things of that nature.

The participant elaborated on NextGen confidentiality by stating that "What is different with ADS-B now is aircraft talk to each other. They are not actually having a conversation, like a session, like ground infrastructure does; but instead of relaying through the ground, it can go from plane to plane now. So it kind of happens on the ground AND in the air."

The participant completed the initial discussion on confidentiality by adding that the data will eventually be publicly accessible

> …if they get clearance; and there is a process to go through; and part of the ADS-B program is actually to help reduce costs by providing that data. There are all kinds of ways to filter it and delay it. Like now, right now – there are systems out there now that provide that data. Not in the detail, but they are all delayed.

Later in the interview, Participant #6 returned to the discussion on confidentiality and added a comparison between ADS-B transmissions and traditional computer networks by stating that some would call the NextGen Active Network "like your home network, but that is not what it is. You are not holding a conversation. You are just

listening. It is strictly broadcast." The participant outlined the differences between ADS –B and a computer VPN connection by stating "Right, and that is the session – an IP session where now you have a tunnel into the system that no one knows about, and they cannot do that with this." The participant closed out the thought with a statement that "When people call it wireless, most people think of their home network or that thing at Starbucks or whatever; and that is not what it is."

Table 8 summarizes the perspectives of all participants regarding confidentiality.

Table 8.

Perspective Synopsis: Confidentiality

Perspective
"Confidentiality does not apply to ADS-B. It is a broadcast system."
"…envisions right data, right user, right time"
"…there is no encryption"
ADS-B messages do not "require some kind of secure communications that you are trying to keep information from getting into the wrong hands"
"If you could encrypt so… the desired users can use it but other people could not that would probably be good to do."
"To get everyone on the same page is extremely difficult if you go encryption or things of that nature."

Integrity

Participant #1

Participant #1 believed that NextGen "does not take specific measures to protect against spoofing or harmful intended interference", but added that "there are significant measures in the system to provide high integrity of data going through the ether, through normal interference." The participant went on to describe the methodologies used by each of the two link technologies proposed for NextGen. For the UAT link which uses Forward Error Correction, if a packet "decodes correctly and passes at FEC" the likelihood of receiving a bad packet "would not be the case for more than 1:100,000,000 messages." For the 1090-ES link which uses legacy technology in the form of a Cyclic Redundancy Check, the participant stated that "you would have a loss of integrity of no more than 1:1,000,000 messages." The participant contrasted this with current Mode A/C transponders that are at best 1:1,000 packets, but asked "is the ATC system unsafe because of this? No, because you get a lot of responses and you do not take drastic ATC action because of any one return from a Mode A/C transponder or basically the ADS-B system or from the radar."

Participant #1 stated that "there is no authentication required" in the proposed implementation of ADS-B in NextGen. The participant clarified this in that "they are not authenticated at all in the sense that I have to authenticate you before I will talk to you or before I will pay attention to your information". The cooperative manner in which ADS-B tracks aircraft suggests that ignoring a message packet from a non-authenticated aircraft could have disastrous consequences. The participant concluded his discussion of proposed ADS-B authentication by illustrating:

> Let us just think about that – and we are certainly not going to take that off the screen because we think that somebody messed up when they installed the 24-bit code into the Mode S transponder of the aircraft. We do not say that is in invalid code, therefore that aircraft must not exist. That is not going to happen. There is no authentication protocol at all by the ground system, nor should there be. You want to know that guy is there, and if there is a mistake in what he is broadcasting, if something is wrong, you want to figure out what it is, and when he lands write him up.

Participant #2

Participant #2 believed that NextGen aircraft, ground station, and satellite transmissions authentication should be considered sensitive information and could not comment on methods employed to insure integrity.

Participant #3

Participant #3 discussed NextGen's ability to guard against existing improper modification or destruction of information in transit stating

> I do not know how you would do that. I mean, the messages – again, are assigned this 24-bit address associated with a particular aircraft, and then you use that information to determine where he is at. I do not know how you would intercept in real time the actual modulation that is going out in space and modify it. That would be difficult to do because just as soon as you change a bit in the data field per the MOPS now, per our standard, industry standard; as soon as you would change a bit in the data field, it would affect the 24-bit parity bits associated with

the address. So the encoding would be wrong, so you would throw that message away.

The participant also expanded on the CRC included in each ADS-B message stating that

> The last 24 bits of the messages are encoded. In the case of ADS-B messages, I think they are all 1's – and I think the way the 24-bit address works, then the actual aircraft Mode S address is part of the data field; but it is still encoded, so if you encoded a bit—let us say you changed a bit in the message, then you would have to know also to be able to intercept exactly at the right point in time when it is received, the 24-bit parity and make sure that it encodes with the data as all 1's.

The participant doubted the likelihood that data integrity could be compromised in practice, stating "It would be pretty difficult to do**."**

Participant #4

Participant #4 believed that the transmission methodologies and error correction techniques used in the airborne portion of the NextGen Active Network would make it difficult to modify or destroy information on the fly stating that

> I do not think there is anything in the airborne side to modify, other than you could potentially go up, and you could be a jamming type of thing where you could transmit a lot of 1090's to the point where the reception and rate would be dropped way down, and you may end up not being able to receive all of the transmissions,

and that the ensuing packet overload could create a "denial of service" effect on ADS-B. This would be most likely within "the 1090 spectrum, that is an issue in some of the high-density areas where you have a lot of aircraft flying, and they are all transmitting." The participant also confirms the dependence on the 24-bit parity CRC method of insuring data integrity by stating that "Parity is really about the only thing that is available."

Participant #4 discussed the issue of authentication within ADS-B by stating "I do not think we try to really authenticate that it is coming from that aircraft, if you are talking air to air – all we are trying to do is a surveillance kind of information." The participant continued to describe ADS-B authentication and a vendor specific enhancement correlating ADS-B and TCAS data by stating that

> There is a sort of authentication from the standpoint that the position that is being reported via ADS-B is the correct position. We do that kind of authentication, and we have TCAS. TCAS is an independent system from ADS-B so if you are within TCAS range (and we do this), we will actually go out there and validate that the position that is coming in is the correct position. If it is not, then we have ways of handling that traffic.

The participant elaborates on the collaboration of air to air message traffic by describing the tracking methodology used as:

> Those are all fixed broadcast messages that we can receive. So we receive that information, and we establish a track to start tracking. Before we take a report and add it to the track that we are tracking the aircraft on, we have a means of using TCAS because we are including ADS-B end function in with the TCAS system; the reason being, of course, is that they both use

1090 reception, a simple way of putting the systems together. So we now can take the capability of the TCAS to interrogate the transponder in that other aircraft, so the transponder is sending me an ADS-B message; but also with TCAS, I can interrogate that transponder and get a reply back; and based on that reply, I can determine its position and relative bearing. So based on that relative bearing and range from my aircraft, I can do a comparison against the reported position to see, and knowing what my position is, I can determine whether that position is valid. My equipment will say – oh, that guy is not what this guy is, so there is no correlating between those two. So I have got a couple of options. One is: I can either throw the data out if it is just spurious; or if it seems to be bogus. Because my TCAS system is going to keep me safe in the environment, and if I have not validated that that guy is providing me good information, then I am not going to use him in any of the applications. Like, for example, if I am doing some kind of spacing application, ADS-B application, I am going to validate the information using that TCAS if that is correct; and if he is validated, then I will use him for that application. And then, of course, there is information that is also provided from, in the transmission itself, that is going to tell me the integrity of the data that is being transmitted as well.

Participant #4 was also aware of the methods in place for insuring ground station integrity, which was described as "a multi-sensor tracker in the ground infrastructure that receives surveillance information from several sources – from the radar…..from the

secondary surveillance radar, from multilateration, and then I think there is a fusion that takes place; and then they do some kind of integrity based on knowing the latency of receiving the data, transmitting the data, all that."

To complete the discussion on data integrity, Participant #4 described methods of insuring the integrity of GPS satellite transmissions in that

> Here you have the GPS system, you have the modem, transponder that is transmitting, and then you have your application sitting somewhere that is receiving this data like that map you were talking about. Well see, it is going to look at all of this information the GPS is creating in terms of the integrity and the accuracy, and it will use that to determine whether the information is good enough to be able to use for that application. And so that, in a sense, is sort of how you authenticate at the end of where you are trying to use this…..the data itself for a particular application.

Participant #5

Participant #5 believed that the design for the ADS-B portion of the NextGen Active Network is designed to provide security with "…integrity built in. There is a 24-bit CRC built into the message that has a probability of detection or probability of false detection of 10^{-6}, I believe, or better. So it does have that built in." The participant continued by including other existing methods stating "There are other things, too, that if the data is really off, it will not be accepted for other reasons, like it transmits latitude, longitude—well, if you receive something for halfway around the world, you know it is hosed up because it is a line of sight, 200- to 300-mile system. And there are other things that you can look at in the data to show it is unreasonable."

In outlining their perspective regarding authentication of ADS-B aircraft transmissions, Participant #5 stated that "If you get a spurt of single transmission or transmissions that the data is vastly inconsistent, then you know there is a problem, but no, you could if you were a terrorist, you could, if you look at that scenario, you could build a little transmitter and put it up at" a local airport. The participant also mentioned an interesting sidelight to the 24-bit ICAO addressing scheme which is individualized to each equipped airframe, noting that the present system does not utilize the information in stating "Any 24 bits would do – other than all zeros and all ones (those are illegal)—but you have 2^{24} - 2 different combinations they can choose."

Participant #6

Participant #6 discussed the designed-in fallback methods within the airborne network to insure data integrity by stating that

> …they have it back into the back end that they have processes in place because they tie what is coming over the air plus secondary surveillance radar – time difference of arrival, and they usually receive different sensors, and they use multilateration so that helps. So if someone is trying to spoof, that will come out. They will identify there is issues going on.

The participant also outlined the evolution of security that will occur as NextGen is deployed

> They need a back-up system, you know – and this can change over time, but not everyone can equip on day 1, so they need to keep all these systems in place on the long term. And then as equipage goes up, then they can readdress; but there

will always be a back-up system of some type. You know the intent is for SSR to always remain in place or some type of backup.

Table 9 summarizes the perspectives of all participants regarding integrity.

Table 9.

Perspective Synopsis: Integrity

Perspective
CRC and FEC insure integrity of 1:1,000,000 and 1:100,000,000 respectively. "No authentication is required."
"That is sensitive"
Tampering "would affect the 24-bit parity bits associated with the address"
"Parity is really about the only thing that is available." "…if you are within TCAS range (and we do this), we will actually go out there and validate that the position that is coming in is the correct position."
"There is a 24-bit CRC built into the message that has a probability of detection or probability of false detection of 10^{-6}"
NextGen will "…tie what is coming over the air plus secondary surveillance radar – time difference of arrival, and they usually receive different sensors, and they use multilateration."

Availability

Participant #1

The participant agreed that it is critical for ADS-B network to insure timely and reliable access to navigational and control information, and stated that

> We have designed the ground infrastructure for a maximum latency from time of receipt of a message that should trigger a report at the service delivery point; and ITT is under very clear design goals there in terms of maximum time it takes, and they are meeting those goals. On the aircraft side, we have a requirement that was in the NPRM, and in a modified form, will be in the final rule on the maximum uncompensated latency, uncompensatable latency from the position source via GPS or something else to the transmission of the ADS-B information out of the aircraft - so timeliness is very important; and there are specific requirements, both in the air and on the ground, to insure it.

Several methods of improving potential ADS-B availability against malicious or intentional interference were mentioned by the participant. The potential techniques to mitigate spoofing within ADS-B mentioned by the participant include using message timestamps to verify distance, triangulation or multilateration of ADS-B messages between multiple ground-stations to verify approximate location, and fusing ADS-B message data with existing radar returns to correlate ADS-B and radar signals and eliminate spurious message traffic. The participant concluded that triangulation and multilateration techniques require ground systems which will initially only occur in high

density areas, but the risk increase with traffic and low density areas by definition have lower traffic and thereby reduced risk.

Conversely, the participant discussed the potential use of the same multilateration, triangulation, or fusing ADS-B and radar data techniques to insure adequate availability. The participant described multilateration as "a technique where the ground infrastructure itself, without secondary surveillance backup" could verify the validity of signals, and suggested its' potential to "of course, also catch spoofers." Regarding early testing of the technique, the participant remarked "No decision has been made, but one place that a serious look has been taken is in the Gulf of Mexico, where we hope to get early operational benefits out of the use of ADS-B – but need to validate ADS-B to insure that we have enough integrity in the non-radar airspace."

Participant #2

Participant #2 agreed that availability "is part of the vision" for the ADS-B portion of the NextGen Active Network to insure that availability by preventing disruptions from intentional and unintentional sources of interference. The participant also concurred that it is critical for ADS-B to insure the timely and reliable access to navigation and control information as part of that vision. The participant also stated that "Today there are many gaps between current networks and the net enabled operational environment envisioned by NextGen" and recommended that the "Implementation of a service oriented architecture with enterprise level security" be utilized to eliminate existing security gaps.

Participant #3

Participant #3 discussed availability by stating that

> There is an industry standard function called hybrid surveillance, which has been released (I forget the DO number of the RTCA document), but it has been released. What it does, if you are a TCAS system, you can interrogate and get a range with secondary surveillance. You can then compare that range to the calculated differential range that you get when you look at your lat/long and the lat/long of the interrogated aircraft from an ADS-B transmission. Again, his lat/long and your lat/long if you know the distance – so you can compare the interrogated range to that range and see if it is within a certain boundary that would qualify it as a threat. And so, in that way, we can check that the information sort of makes sense.

Participant #3 discussed the potential of interfering with NextGen by broadcasting ADS-B messages for non-existent aircraft by stating

> You might, for instance, send traffic with a lat/long, and maybe what you are getting at is - someone else could send out traffic with a different lat/long to show that someone is there that is not there, I guess. I am not sure what kind of a problem would result from that, even if that were to happen, because… Okay, so you are going to see some additional airplanes out there.

The participant injected that hybrid surveillance would eliminate the threat, because "if that is going on, someone could direction-find the guy where he is and shut him down. So, hey, by the time he made his threat and maintained interference, someone would find him."

Participant #3 also stated that spoofing would be reduced or eliminated based on software within their systems which correlate ADS-B and TCAS transmissions. The

participant stated that "it is doing a secondary surveillance range. This guy says he is at this range. I am interrogating him, and nobody is answering." The NextGen system's ability to eliminate the uncorrelated information would prevent bad data from effecting flight paths.

Participant #3 summed up their perspective on NextGen availability by stating that:

> If you are talking about, say tracking another airplane, it is a constant update; so we are looking for data each second using that form where we call tracks – and so the data has to be continually there in order to maintain a track. So, you can speculate about all kinds of disruption, but I mean, that is how it works. For instance, if you lose data for two or three scans in a row, two or three seconds in a row; you are still going to maintain a track; and even if the data's coming through intermittently you will filter and associate with that 24-bit address – and you will maintain and track for that aircraft. So some amount of loss of data can occur and still maintain a track. I guess that is the positive side.

Participant #4

Participant #4 did not believe that the proposed NextGen network insures availability by preventing disruptions from intentional or unintentional interference, and stated "Other than just the check of the data that is being transmitted; there is nothing, I do not think, that really prevents the interference, unintentional interference that I am aware of. And again, I am just talking about the 1090 link." The participant elaborated on how the airborne network links were developed commenting that

> The way ADS-B came about is an evolution, if you will. With the secondary surveillance radar and how that works, which was an evolutionary replacement of the primary radar that was doing the painting. Now you have secondary surveillance, which now takes advantage of the transponder that is on the aircraft. It can interrogate that transponder or transponder reply; and it will, of course, give you a position or relative position in data. That used two sets of frequencies, 1030 and 1090, specific frequencies. The 1030 was used as the interrogation; 1090 is the frequency that you replied on. And so, the evolution continued; and now we got into ADS-B, and we said….Ah, well; we have a transponder on the aircraft. All we have to do is hook up a couple of positional sources, and now we can transmit its position on a broadcast basis; and we will use the 1090 transmission that is already on the aircraft.

Additional elaboration by Participant #4 outlined a secondary concern in the selection of the 1090-ES data link and stated "It is a single channel, right, because everybody is broadcasting. Of course, with the mode S transponder, everybody has an address; and so there are mechanisms to go up and, based on interrogations, you can have one call and get everybody to reply; or you can communicate just directly with one aircraft or another; but you are only using that one frequency." The participant later continued this train of thought and added that

> The ARC has come up with, some of the concerns that they have are around how much 1090 transmissions are occurring. Single channel, you have lot of transmissions out there, so you could get into a saturation point at high-volume airports. You get into a saturation point, and then; so what begins to do is the

> acceptable rate of receiving information starts to go down; your range of receiving information goes down; and ultimately, you get to a point where your reception rate is… you cannot do anything with it. So that is a potential problem. I mean, it is even a potential problem of somebody not trying to do it but just because of the virtue of too much traffic on a single frequency trying to do too much. But, of course, the industry is looking at ways of at least trying to resolve that situation.

The participant also explored potential solutions to the problem and explained that

> There are some technologies that are going forward. We have some technology that we can offer, but there are things that they can do to go in and reduce, that could get rid of secondary surveillance radar. They could go to hybrid surveillance; use hybrid surveillance, which is melding TCAS and ADS-B, so there are things that can be done to reduce that.

Participant #5

Participant #5 noted that the proposed NextGen Active Network does not insure availability from intentional or unintentional interference by stating that "if somebody wanted to jam it, they could. It is not like a spread spectrum type of thing where it is anti-jam resistant." The participant also commented on the criticality of timely and reliable network access and stated that "a lot of the applications are, you know, time sensitive. …some of our other applications are merging spacing, so the data has to be received within a timely manner, or else you are not going to get valid data. There are specifications in the MOPS that say you have to generate a report within a certain length of time after receiving it, so there are requirements to ensure you have adequate latency."

Participant #6

Participant #6 asserted that NextGen transmissions will maintain availability through the same authentication methods now in use which they described as "the same kind of error checking that we just talked about is generally how that is done right now" and "There are flight plans in place, so there is a procedure that is going on now that is going to stay, and that is taken into consideration when they are comparing messages they are getting and secondary radar inputs. That is how they discover the inconsistencies."

Participant #6 continued the discussion of availability by asserting that the FAA regulations

> …have the procedures in place that if that happens, they revert to the way they do business now. I mean – if someone jams something, they have to just find the source. They know that as the equipment evolves, it is going to be able to deal with that stuff better, but it is usually most of the problems like that are dealt with by procedures. ADS-B is not going to relieve the pilot of any of his duties, so he is still responsible to get the job done, even though there could be issues with it.

While this does not provide assurance that the NextGen air traffic control system will remain constantly available, the participant highlighted the fact that there is a fallback plan which utilizes legacy methods and technologies to allow continued operations at current standards.

Table 10 summarizes the perspectives of all participants regarding availability.

Table 10.

Perspective Synopsis: Availability

Perspective
"…timeliness is very important; and there are specific requirements, both in the air and on the ground, to insure it."
"Today there are many gaps between current networks and the net enabled operational environment envisioned by NextGen."
Air to air authentication is insured by hybrid surveillance.
"…use hybrid surveillance, which is melding TCAS and ADS-B data"
"It is not like a spread spectrum type of thing"
Existing error checking, with a fallback to legacy flight procedures

Additional Comments

Participant #1

Participant #1 remarked that industry, education, and government should improve their working relationships to address security assessments by stating that:

> This is an area that, on a government-wide basis, is very much open for improvement; and that improvement would rebound into the ADS-B ground infrastructure backhaul. It has been very difficult for people who are implementing information services on the civil side of the government to get appropriate threat assessments, appropriate classification of data they are doing, and to know with confidence what they need to do. Within each agency you tend to have, what I call *security-niks*; and whether or not there is a problem, we need better security to defeat the non-problem. This tends to obscure the fact that the people beating the drum are the special *security-niks* within the various agencies; tends to obscure the situation. It tends to become a rice bowl issue as opposed to getting looked at strictly on the merits. It is unfortunate that we have maneuvered ourselves into this situation. Then if a responsible program manager such as the ADS-B program manager consults with NSA, it is not easy for NSA.

Participant #1 acknowledged that the *security-niks* are clearly experts, but questioned whether they have the staff or the manpower to effectively respond to requests

for threat assessments. "We need good threat assessments in terms of risks and exposures compared to risks and exposures that we take today. We need more comparative security assessments than de novo, ground up, out of a book, security assessments. We need to be able to take credit for the fact that we have been accepting a degree of risk and things have been going well -- and just look at how things are different, and to the degree they are different; take that into account in terms of increasing our security and privacy concerns."

Participant #2

Participant #2 recommended that NextGen "participate in COI activities and in data and standards related consortiums" to address the security needs of the industry and successfully feed the pipeline of intellectual capital."

Participant #3

Participant #3 compared the message standards employed by ADS-B to existing computer network standards and stated that

> If you look at the information rate associated with this system and try to apply Internet standards, there is a high degree of overhead on the data that is being transmitted. We are already, because of the industry standards, we are already using almost all the bits for information and/or this 24-bit parity, so there are not a lot of bits left over to go do like a TCP/IP protocol with all that overhead, so you were asking is there a need for the overhead? I guess my answer is that we are following the industry standards the way they are, and we have used all the information bits.

Participant #4

Participant #4 rejected the need for additional security within the airborne portion of the NextGen Active Network by stating that

> …again, this is based on my perspective; and I guess it would be depending on what the threat would be. I guess, if I look at it from the standpoint that if I had a means to gather data and interject it into the system that could create havoc, then I would say yeah, you are probably at risk. But as long as you have security to not allow that to happen, then the airborne side, I do not think, is going to require that. When we start going, and that is the air to ground, getting into the ATC automation. When you are looking from air to air, as long as you have a way to validate or do that authentication that we were talking about before, then you are probably okay as well in terms of any threats that may happen. But again, it would depend on the type, the threat that you are looking at specifically. But based on the way I see things today and how they want to use it, I do not think there is a need for it.

Participant #5

Participant #5 questioned the need for additional security within the airborne portion of the NextGen Active Network by stating that "it really was not built as a secure-type link. I mean, is it necessary? I do not know." He/she added "… from a collision avoidance standpoint, it is not currently used for collision avoidance. There is an independent system for that. TCAS is independent" then completed the perspective by stating that "It is likely if somebody disrupted ADS-B, they are not likely going to cause

a collision if you have an airplane that is equipped with TCAS because that works independently of ADS-B and would detect that – so I am not sure how to answer that."

The participant's recommendation to eliminate some of the security gaps includes merging ADS-B and TCAS data within airborne systems. The participant described the potential benefits stating

> Our TCAS performs both the ADS-B end function as well as the collision avoidance function. That does its own checking of ADS-B versus, you know, the secondary surveillance replies; so it, in fact, does that already, and TCAS uses secondary surveillance radar data, which has been deemed to be more accurate or more reliable than ADS-B data. So that is already done for airborne systems if you have a TCAS. The ground stations probably could do that, too, and should do that because most 1090/ADS-B systems are mode S transponders with an ADS-B function put in it, so it does both the secondary surveillance radar as well as ADS-B. So the ground station, radar ground stations definitely can and should authenticate or verify that both are within the tolerance of radar.

Final comments from Participant #5 were directed at the rationale between the 1090-ES and UAT platforms. The participant stated that

> I do not think any of the OAMs are talking about equipping with UAT. The, you know, transport airplanes. The Boeing or Airbus, I do not think they are looking at UATs. There are some things with UAT that do not make a lot of sense because if you are flying in IFR conditions, most places you have to have a transponder; so it does not make sense to have a transponder and a UAT system when you can have just the transponder that does ADS-B. So there is some limit.

> It is kind of not going to make a lot of sense in a lot of cases. Why should you put a second system on your airplane when you can… Yeah, a lot of airplanes have just the ATCRBS transponders, which do not do ADS-B; but they can replace them with a mode S with additional cost.

The participant stated that the 1090-ES system "does both instead of having two different systems and maybe two different antennas." The participant closed with a thought regarding 1090-ES versus UAT equipping for "as long as FAA is going to require secondary surveillance radar, which I think they are near term; then a lot of times, it just does not make sense to put in UAT."

Participant #6

Participant #6 took time to correlate the NextGen communications with existing FAA computer network standards and stated that

> FAA is very rigorous on their FISMA and going through SCAP for their ground infrastructure. They are more regimented than, I think maybe DOD is worse, but that is about it. They do a very good job, it is very diligent. There is separation of roles and responsibilities. I have done a lot of CNA work for DoT, FAA, and different places; and FAA is, just my experience, so far is the best one about getting it done correctly, consistently, and tracking it. It is not a paper exercise.

The participant then expanded the thought regarding computer network standards into the airborne portion of NextGen by stating that

> Because a lot of FISMA, when it ends up in the NIST requirements, the air to air it applies but it does not at the same time because you are not really creating communication sessions. Most of FISMA is about creating a session and getting

in and doing damage, you know, get in and control the system; and in the air to air, you can spoof and jam, but you really cannot go in and modify things.

The participant expanded on the discussion by adding "it is kind of like you are going under the power lines of the AM radio kind of thing. You cause an issue with the signal, but you are not going to create damage to the system if everyone follows their procedures."

Participant #6 briefly discussed the potential of using ADS-B as a targeting device for terrorism, and responded that "the issue with that is – you can do that now. You do not need ADS-B. People are bringing up all these creative ideas, but they do not realize that, just the information, it is already been out there. It is just that ADS-B makes it more efficient."

Thematic Analysis of Participants

The findings in this study involved the examination of the selected stakeholders' input related to the research questions developed in Chapter 1 of:

1. How does proposed ADS-B network design for the NextGen air traffic control system compare to government and commercial industry network security standards?
2. How does the ADS-B portion of the proposed NextGen network design perform when faced with common computer network threats such as Denial of Service, Session Hijacking, and Network Eavesdropping?
3. How does the ADS-B portion of the NextGen network model insure confidentiality, integrity, and availability?

and the Interview Question Guide shown in Appendix C. The primary focus areas developed through a review of the literature include the three primary security objectives outlined in the Federal Information Security Management Act of 2002 of confidentiality, integrity, and availability.

Additional comments based on the participants' unique perspectives which were either peripheral to or outside of the direct focus of this study were captured for direct application where possible and for potential future research where there less direct correlation occurred.

Confidentiality

The participants' opinions regarding the confidentiality capabilities and requirements within the ADS-B portion of the NextGen Active Network shared a number

of common themes. Five of the participants, or 83% of the sample, noted that there is no encryption used in the airborne portion of the network and therefore anyone with a capable receiver may capture the information being transmitted in the clear. Four of the participants, or 67% of the sample, commented that ADS-B transmissions are a broadcast medium as opposed to the handshake, session, or connection protocols utilized between transmitter and receiver within normal computer networks, and therefore should not be evaluated on the same criteria. Three participants, or 50% of the sample, also mentioned that harmonization between U.S. and world standards would make the use of encryption to insure confidentiality problematic, as the distribution of shared keys or certificates to thousands of aircraft would be time consuming and difficult. Two of the participants, or 33% of the sample, also believed that it is the intent that aviation data only be released to the aviation community and not the world at large. One participant summed up several comments which focused separately on flight safety by stating that the location of any aircraft in the National Air Space must not be a secret, therefore confidentiality was not necessary or desirable.

Additional comments surrounding confidentiality primarily surrounded a perceived need by some aircraft users for anonymity, which is provided in the UAT link, but not currently available under the 1090-ES standards. In this case, confidentiality is not a security issue, but a privacy issue and does not fall within the purview of this study.

Integrity

The participants also contributed similar information under themes surrounding data and network integrity. Five of the participants, or 83% of the sample pointed to the CRC, FEC, and/or 24-bit parity methods built into the UAT and 1090-ES standards to

insure integrity. Three of the five mentioned statistics indicating a maximum error rate for the UAT data link using FEC at 1:100,000,000 packets, and the error rate for the 1090-ES data link using CRC at 1:1,000,000 packets. The sixth participant declined to comment on integrity as they deemed the topic too "sensitive" for this potentially public forum. Three of the participants, or 50% of the sample, cited secondary surveillance methods of insuring data integrity including utilizing TCAS active ranging to verify ADS-B targets. Three participants also highlighted the potential of using TDOA, multilateration, and other reasonableness checks to validate the integrity of inbound data; and discussed the algorithms used in GPS which are passed to ADS-B along with position data in the form of validity and integrity values.

Three participants also mentioned that ADS-B was *spoof-able*, but that both aircraft and ground equipment should be able to sort out the real targets from bogus ones using SSR, TCAS, multilateration, triangulation, and/or fusing primary radar and ADS-B data to correlate sources. Three other users commented on their belief that losing one or several ADS-B messages would not significantly impact the safety of the system, as messages are transmitted once every second and the onboard computer systems that manage the data develop a track for each aircraft based on multiple successful packets. Spurious messages would likely be discarded as out of range or non-correlated against other information sources.

Availability

Common themes also emerged within the study of NextGen network availability. Four of the participants, or 67% of the sample, cited specific concerns regarding the vulnerability of ADS-B to Denial of Service attacks within the 1090-ES data link which

could be caused by increased traffic in high-density airspace such as the northeast corridor or at any of the major airports including Atlanta, Chicago, Los Angeles, or Dallas-Fort Worth. The same vulnerability could also be exploited by malicious sources, but either case could effectively hamper the use of ADS-B for spacing and separation purposes and force facilities to revert to legacy radar and radio methods for controlling air traffic during peak traffic periods or attack. The same four participants cited that both GPS and ADS-B signals, on either data link, were susceptible to malicious interference through jamming although most agreed that sources of the interference should be able to be quickly identified and removed. Three of the four participants also mentioned that both 1090-ES and UAT operate on single frequencies which are potentially susceptible to jamming, and suggested that a spread spectrum methodology could reduce the vulnerability.

Four participants also cited multiple methods which are included in the NextGen Active Network design to insure availability. The methods included fusing ADS-B and backup radar data, multilateration, TDOA, invoking hybrid surveillance techniques, managing system latency, and/or SSR to correlate targets within both airborne and ground-based systems.

Three of the participants, or 50% of the sample, believed that the design of NextGen and the differences between requirements for public airspace and computer networks precluded the application of traditional computer network measures of availability. The differences between connection-based computer networks such as the wireless network at Starbucks versus the broadcast nature of ADS-B were again highlighted. The ADS-B messages used within the NextGen Active Network are

connection-less in nature and broadcast to all aircraft and ground stations within range. One user reminded aviators that the potential of lost or gained system availability from NextGen did not relieve the pilots from their responsibilities for safe flight.

Financial Impact

The financial impacts of NextGen were split by demographics. The two government employees cited the cost savings purported by the NextGen implementation including more efficient spacing, trajectory management, and safety data. The three engineers working for avionics manufacturers cited the sales of new ADS-B systems as the fleet is equipped for NextGen. The final respondent did not see an immediate impact to their consulting practice, but seemed to see business as a continuation of ongoing advisory tasks. Table 11 summarizes the perspectives of all participants regarding the financial impact of NextGen on their environment.

Table 11.

Perspective Synopsis: Financial Impact

Perspective
"…something I work on, but there is no financial impact other than the fact I provide consulting services"
"DoD stands to experience cost savings associated with more efficient use of the National Air Space."
"…obviously we are going to sell products for ADS-B, and we have already announced that."
Increased business as aircraft are equipped.
"It is good for us usually as long as it is 1090."
"In the long run – well, what they are trying to do is make the airspace more efficient and safer; so in the long run, it could save you money."

Government, Industry & Education Partnerships

The individual perspectives on this topic were quite varied. One recommendation suggested that the three entities develop better methods of measuring information security based on context and threat based models weighed against currently acceptable risks. Other participants recommended that academia engage with government and industry in consortiums such as RTCA, ICAO, ARC, and participate in Community of Interest groups. One participant specifically cited the FAA's use of MIT as a technical resource when internal resources do not have specialized capabilities required for

programs such as NextGen. Table 12 summarizes the perspectives of all participants regarding government, industry, and education partnerships surrounding NextGen.

Table 12.

Perspective Synopsis: Government, Industry & Education Partnerships

Perspective
"I have long hoped that the government would come up with a better way of looking at information security that is contextually based – not only in contextually based and threat based – and also look at the risks that have been acceptable in the past."
"Participate in COI activities and in data and standards related consortiums."
"We hire from a number of colleges and universities."
Supporting government and industry partnerships with industry standards and rulemaking group memberships. Supporting industry and academic partnerships by participating in this study.
"…RTCA is where you get a lot of synergy… You have government, industry; a lot of times, the academia like MIT, they get hired by the FAA as their technical arm"
"…we have a lot of industry working on this program. At times they are. I mean, I am not sure of all the people working on the program. I mean, it really goes through a large group of people, you know, subject matter experts, and things."

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The purpose of this study was to identify and describe the risks inherent to the active network within the ADS-B portion of the proposed NextGen system and compare the proposed enterprise architecture against current best practices in computer network security while answering the following primary research questions:

1. How does proposed ADS-B network design for the NextGen air traffic control system compare to government and commercial industry network security standards?
2. How does the ADS-B portion of the proposed NextGen network design perform when faced with common computer network threats such as Denial of Service, Session Hijacking, and Network Eavesdropping?
3. How does the ADS-B portion of the NextGen network model insure confidentiality, integrity, and availability?

The conclusions regarding the questions that follow are meant to be used to enhance the development of the future NextGen air traffic control system. They discuss the need for additional security considerations in light of the similarities and differences between NextGen and industry standard computer networks.

NextGen Comparison to Network Security Standards

Based on this research, there are both significant similarities and differences between the NextGen Active Network and industry standard computer networks. Both the ADS-B and 802.11 computer networks operate in a wireless environment. Both are designed to move information between local devices, though the ADS-B devices may cover 200-300 miles at altitude where the 802.11 computer networks are designed to cover a range of 200-300 feet. Both have methods of insuring a high level of data integrity using FEC, CRC, 24-bit parity, or MAC codes. At this point the similarities diverge, as the missions of the two networks are markedly different.

1. The computer network has designed-in encryption to insure that only authenticated computers may access the network and receive information. The ADS-B network is designed without encryption or authentication to insure that every ADS-B equipped air or ground vehicle is able to receive information regarding other vehicles within range. This difference in ADS-B is a safety consideration, but does raise privacy issues within general aviation.

2. The computer network primarily transmits information between two known IP addresses, or very occasionally may transmit to multiple known IP addresses if it is sharing some form of streaming media. Computer transmissions often require a handshake or connection that generally results in acknowledgement by the receiving computer. The ADS-B network primarily broadcasts to an unknown number of receiving vehicles and/or ground stations, expects no acknowledgement and requires no handshake or connection.

3. Newer computer networks transmit and receive using a spread-spectrum methodology that can be difficult to jam because it operates on multiple frequencies simultaneously. The ADS-B network operates two data links on different frequencies, but it is not intended that an ADS-B aircraft or ground vehicle would be equipped with more than one of the frequencies.

4. Computer networks insure availability through authentication, denying access to devices which cannot successfully authenticate. The ADS-B network insures availability through repeated transmissions at one second intervals, and avoids device authentication which would have a potentially negative impact. It is critical to know if an aircraft is in your vicinity or on a collision course whether or not it has been properly authenticated by the NextGen network.

Based on the mission differences between the two networks, several of the computer network standards pertain, but in a different manner within the ADS-B environment. Maintaining encryption across the envisioned global fleet of ADS-B equipped aircraft and vehicles would require managing periodic updates to encryption keys. This process could be self-defeating because either everyone has the keys or the keys are never changed, and in both cases the encryption is rapidly cracked or widely knowable. The 1090-ES data link also has bandwidth limitations that would be further impacted by encryption overhead.

NextGen Performance Against Common Threats

The ADS-B portion of the proposed NextGen Active Network has both strong points and weaknesses when faced with common computer network threats. When faced with a Denial of Service attack, the UAT data link is fairly robust and more difficult to overrun, however, the 1090-ES data link contains not only ADS-B but other transponder traffic including Mode S and legacy ATCRBS traffic. In areas of high traffic density, the number of messages received on the 1090 MHz frequency may be more than the total bandwidth available and packet loss will occur. The Denial of Service attack could also be induced through malicious interference which would effectively disable ADS-B in localized vicinity of the attack. NextGen design specifications call for the 1090-ES data link to be used primarily by 19-seat or larger transport aircraft, and/or aircraft operating at or above 24,000 feet. The weakest data link in this case is supporting aircraft with the largest payloads and therefore the highest need for safety.

Session Hijacking is much more difficult to induce in an all-RF environment such as the airborne portion of the NextGen Active Network. None of the engineers interviewed could determine a reasonable method to induce this effect because the transmissions on ADS-B are not connection or session based. There is a risk that ground communications which traverse computer networks could be effected, however, they are outside of the scope of this study.

The concept of Network Eavesdropping takes on a life of its own in the NextGen Active Network. While computer networks are designed to insure that only the intended recipient of a message is able to receive and interpret it, the ADS-B network is designed to insure that all ADS-B equipped vehicles are able to receive and interpret all messages.

The proposed design has the unfortunate side effect of also allowing reception of all ADS-B traffic by anyone with an appropriate radio and decoder. The raging debate in the aviation community surrounds the ability of the public to obtain ADS-B data and know all aircraft tracks and destinations. This becomes a sensitive issue with general aviation aircraft used for personal or corporate travel. Several participants discussed the use of anonymous mode, which is only presently available on the UAT data link, to allow individual aircraft to transmit a VFR-like code rather than their 24-bit ICAO designator which may be mapped back to the aircraft's tail number. This is not truly a security issue, but an issue of privacy.

NextGen Compliance with FISMA Objectives

As stated in the two previous sections, there are points at which the NextGen Active Network and computer networks both correlate and diverge.

1. Confidentiality is neither desirable nor implemented within the ADS-B environment because the designed broadcast medium only works when each aircraft understands the position and track of all other aircraft within the vicinity. Conversely, the lack of confidentiality can potentially expose the movement of all aircraft to the public, which could use the information to track corporate movements, personal flights, etc.
2. Data integrity is designed in to both UAT and 1090-ES data link standards. UAT utilizes forward error correction which results in a 1:100,000,000 (or 10^{-8}) error rate. The 1090-ES data link uses a cyclic redundancy check which results in a 1:1,000,000 (or 10^{-6}) error rate. Both data link standards are susceptible to spoofing if messages are transmitted from a malicious source.

3. Unlike computer networks which can be fairly tolerant to the rate at which messages are received and processed, timeliness as measured by latency for the NextGen network is critical to accurate functionality. A delayed message in a computer network might cause information to appear slower than you would like or induce jitter in a voice over IP telephony connection, but will not likely misrepresent your position in reference to another aircraft traveling toward you at a high velocity. NextGen has set very high standards to minimize latency within ADS-B. Unfortunately, other measures of availability within the ADS-B network have susceptibilities that are less prevalent in computer networks. The ability to jam the 978 MHz and 1090 MHz frequencies that UAT and 1090-ES occupy, or simply overrun the 1090-ES data link with legacy transponder traffic place the system at some risk for loss of availability by a Denial of Service attack. The inability of ADS-B alone to determine the authenticity of a message could allow spoofing to clutter the CDTI with fictitious aircraft.

Security Recommendations

To address confidentiality concerns, one must weigh the real impact on free commerce or perceived loss of personal freedom against the safety of travel within the national airspace. Under no circumstance should an aircraft be invisible to ATC or other aircraft while in flight, with the possible exception of special military or state flights such as Air Force One. Virtually all of the information which several groups have requested not be disclosed are already freely available on the Internet at sites which utilize existing legacy technologies. This will likely be a long hard-fought legal battle between opposing

interest groups, but in the end should have no functional impact on the security of the NextGen Active Network.

To address integrity concerns, in particular those induced by the possibility of spoofing, both airborne and ground-based systems should employ multiple techniques to insure that each aircraft appearing on ATC and CDTI screens actually exist, and conversely, that each aircraft which is occupying airspace is accurately reflected within NextGen. Multiple methods can and should be employed to assure integrity in this context including fusing backup radar signals or hybrid surveillance with ADS-B targets to prevent spoofing, the use of multilateration or triangulation using multiple ground stations to confirm that an aircraft's actual position correlates with their transmission point in space, and the correlation of airborne ADS-B and SSR (and/or TCAS) information to confirm radar range against the ADS-B broadcast position.

Existing plans discussed in the recent ARC report on the FAA Notice of Proposed Rulemaking for ADS-B (ADS-B Aviation Rulemaking Committee, 2008) outline a requirement for maximum acceptable latency within the NextGen Active Network and will effectively address the timing issue. Remaining issues revolve around the availability of inbound satellite signals for GPS positioning, and inbound aircraft and ground signals for ADS-B which reside on two frequencies. None of the ADS-B sources are impervious to jamming. GPS data relies on receiving data from a number of satellites and determines data integrity based on the quantity and quality of sources. UAT and 1090-ES can both be jammed by other transmissions on their dedicated frequencies, but in all cases the symptoms would be quickly noticed and transmitter locations could be easily tracked down.

One integrity concern that is partially addressed earlier in this section warrants additional concern and recommendation. Perhaps the greatest potential security threat to cooperative surveillance systems such as ADS-B and NextGen is that some aircraft just will not *cooperate*. Whether the aircraft is being flown by Jihadists seeking to reign down terror on the evils of America, a drug runner wishing to escape detection, or just a poorly maintained aircraft, there is a grave risk in relying strictly on cooperative surveillance. Some proposals have suggested that eliminating primary radar systems could eliminate more than $300 million per annum in operating costs (ADS-B Aviation Rulemaking Committee, 2008). I would strongly advocate retaining secondary ground-based radar capabilities in at least all high density areas where the risks of accidents and consequences are greatest.

Final Recommendations

Unlike foreign ADS-B implementations, the U.S. program has selected multiple standards for data communications within NextGen. This duality causes increased costs by requiring additional complexity in the ground stations to include transceivers which convert and retransmit UAT information onto the 1090-ES frequency and vice versa. It prevents smaller U.S. aircraft which would be equipped with UAT from integrating with ADS-B systems if flown out of the national airspace. It also prevents 1090-ES aircraft from taking advantage of some of the additional applications which will be available only on UAT including FIS-B and others not yet envisioned.

Recognizing that 100% of the large commercial operators have already equipped their aircraft by mandate with 1090-ES based transponders and TCAS, the aviation community could be throwing good money after old technology by re-using the lower

bandwidth 1090-ES solution for our largest carriers instead of selecting the higher bandwidth and higher capability UAT solution. This issue is exacerbated by the number of countries controlling large geographic areas which have already published standards selecting 1090-ES as a common standard for ADS-B. Perhaps the best recommendation for the present is to continue equipping aircraft with the present 1090-ES and UAT solutions over the next 10-15 years while building out the complete ground infrastructure, then plan on migrating both frequencies to a single platform solution built around new high-bandwidth, spread spectrum, jam resistant technologies, that will undoubtedly exist by that point in time. By planning this far in advance, the FAA, ICAO, Eurocontrol, Australia and other pivotal countries may be persuaded to embrace a final common standard worldwide.

Future Research

A number of the topics covered by this research have left new questions discovered and yet unanswered. Research opportunities within the realm of aviation data security abound and will continue to expand with the development of NextGen, the discovery of new security threats, and the expansion of technology into aerospace industries. Immediate research interests include:

1. Research into newer, more cost effective airborne radio and processing technologies to allow more rapid equipage of aircraft to the NextGen standard.
2. Research into methods to relieve congestion and improve bandwidth on the 1090-ES frequency spectrum.

3. Research into common software development and certification standards for EFB's and the growing amount of flight deck automation.
4. Research into solutions to prevent distribution of privacy information beyond the aviation community of interest and other parallels with Digital Rights Management.

The ability to maintain the security of our airspace and our nation against the growing internal and external threats may well define America's ability to not only prosper in the future, but remain a sovereign nation providing leadership and opportunity to others worldwide. Although this study selected one well-defined segment of NextGen security, continuing research in all areas is not only recommended but imperative.

Final Conclusion

Is the sky falling? No, but based on this research there are several areas within the proposed NextGen Active Network which could be improved to reduce the risks which are addressed by computer security standards.

REFERENCES

ADS-B Aviation Rulemaking Committee (2007). *Optimizing the Benefits of Automatic Dependent Surveillance - Broadcast*.

ADS-B Aviation Rulemaking Committee (2008). *Recommendations on Federal Aviation Administration Notice No. 7-15, Automatic Dependent Surveillance - Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Notice of Proposed Rulemaking*.

Cisco (2007). Threat Control and Containment: New Strategies for a Changed Threat Landscape. 10. Retrieved February 21, 2009, from http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/net_implementation_white_paper0900aecd805bae31.pdf

FAA (2008). FAA Surveillance and Broadcast Services Retrieved 5/20/08, 2008, Retrieved February 21, 2009, from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/enroute/surveillance_broadcast/

Flt Tech Online (2009). Garmin Adds More Traffic Display Options to ADS-B Transceiver Retrieved 02/21/2009, 2009, from http://www.flttechonline.com/Current/Garmin Adds More Traffic Display Options to ADS-B Transceiver.htm

Gardner, G. S. (2005). *Evidence toward an expanded international civil aviation organization (ICAO) concept of a single unified global communication navigation surveillance air traffic management (CNS/ATM) system: A quantitative analysis of ADS-B technology within a CNS/ATM system.* Unpublished Ph.D., Northcentral University, United States -- Arizona.

Gay, L. R., Mills, G. E., & Airasian, P. W. (2006). *Educational research: competencies for analysis and applications* (8th ed.). Upper Saddle River, N.J.: Pearson Merrill Prentice Hall.

ICAO (2008). *ADS-B and Security Issues*. Paper presented at the The Seventh Meeting of Automatic Dependent Surveillance - Broadcast (ADS-B) Study and Implementation Task Force (ADS-B SITF/7).

Jochum, J. R. (2001). *Encrypted Mode Select ADS-B for Tactical Military Situational Awareness.* Massachusetts Institute of Technology, Boston.

Joint Program Development Office (U.S.) (2007a). *Enterprise Architecture V2.0 for the Next Generation Air Transportation System*. Retrieved February 21, 2009, from www.jpdo.gov/library/EnterpriseArchitectureV2.zip.

Joint Program Development Office (U.S.) (2007b). *Security Annex Concept of Operations for the Next Generation Air Transportation System - Version 2.0*. Retrieved February 21, 2009, from http://www.jpdo.gov/library/NextGen_Security_Annex_v2.0.pdf.

Joint Program Development Office (U.S.) (2008a). *A Comparative Assessment of the NextGen and SESAR Operational Concepts*.

Joint Program Development Office (U.S.) (2008b). *NextGen Integrated Work Plan Version 1.0*. from http://www.jpdo.gov/iwp.asp.

Joint Program Development Office (U.S.) (June, 2007). *Concept of Operations for the Next Generation Air Transportation System - Version 2.0*. Retrieved February 21, 2009, from http://www.jpdo.gov/library/NextGen_v2.0.pdf.

JPDO (2007a). *Enterprise Architecture V2.0 for the Next Generation Air Transportation System*. Retrieved February 21, 2009, from www.jpdo.gov/library/EnterpriseArchitectureV2.zip.

JPDO (2007b). *Security Annex Concept of Operations for the Next Generation Air Transportation System - Version 2.0*. Retrieved February 21, 2009, from http://www.jpdo.gov/library/NextGen_Security_Annex_v2.0.pdf.

JPDO (June, 2007). *Concept of Operations for the Next Generation Air Transportation System - Version 2.0*. Retrieved February 21, 2009, from http://www.jpdo.gov/library/NextGen_v2.0.pdf.

Keizer, G. (2008, September 16, 2008). Microsoft looks to spread secure software expertise. *Computerworld*.

Lester, E. A., & Hansman, R. J. (2007). *Benefits and Incentives for ADS-B Equipage in the National Airspace System* (No. ICAT-2007-2). Cambridge, MA: MIT ICAT (International Center for Air Transportation, Massachusetts Institute of Technology).

Microsoft (2009). The Microsoft Security Development Lifecycle (SDL) Retrieved February 21, 2009, from http://msdn.microsoft.com/en-us/security/cc448177.aspx

National Institute of Standards and Technology (U.S.) (1994). *FIPS PUB 191 - Guideline for the analysis of local area network security*. Gaithersburg, MD: Dept. of Commerce.

National Institute of Standards and Technology (U.S.) (2002a). *SP 800-30 Risk Management Guide for Information Technology Systems*. Retrieved February 21, 2009, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

National Institute of Standards and Technology (U.S.) (2002b). *SP 800-48 Wireless Network Security*. Retrieved February 21, 2009, from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

National Institute of Standards and Technology (U.S.) (2003). *SP 800-42 Guideline on Network Security Testing*. Retrieved February 21, 2009, from http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

National Institute of Standards and Technology (U.S.) (2004). *FIPS PUB 199 - Standards for security categorization of federal information and information systems*.

National Institute of Standards and Technology (U.S.) (2006). *SP 800-53 Recommended Security Controls for Federal Information Systems*. Retrieved February 21, 2009, from http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

National Institute of Standards and Technology (U.S.) (2008). *SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories*. Retrieved February 21, 2009, from http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf.

Olive, M. L. (2001). *Efficient datalink security in a bandwidth-limited mobile environment - an overview of the Aeronautical Telecommunications Network (ATN) security concept*. Paper presented at the Digital Avionics Systems Conference.

RTCA Inc. (Firm) (2002). Minimum aviation system performance standards for Automatic Dependent Surveillance Broadcast (ADS-B) (pp. 1 v. (various pagings)). Washington, DC: RTCA, Inc.

RTCA Inc. (Firm) (2006). Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance - Broadcast (ADS-B) and Traffic Information Services - Broadcast (TIS-B).

Sampigethaya, K., Poovendran, R., & Bushnell, L. (2008). *Security of Future eEnabled Aircraft Ad hoc Networks*. Paper presented at the The 26th Congress of International Council of the Aeronautical Sciences (ICAS). Retrieved February 21, 2009, from http://www.ee.washington.edu/research/nsl/papers/atio-08.pdf

United States Congress Committee on Government Reform, E-Government Act of 2002, H.R. 2458 C.F.R. (2003).

APPENDICES

APPENDIX A

IRB APPROVAL FORM

Oklahoma State University Institutional Review Board

Date:	Wednesday, November 12, 2008
IRB Application No	ED08161
Proposal Title:	A Security Risk Analysis of the Data Communications Network Proposed in the NextGen Air Traffic Control System
Reviewed and Processed as:	Exempt

Status Recommended by Reviewer(s): Approved Protocol Expires: 11/11/2009

Principal Investigator(s):

Robert G. Wood
317 S. Chardon Dr.
Mustang, OK 73064

Mary Kutz
319 Willard
Stillwater, OK 74078

The IRB application referenced above has been approved. It is the judgment of the reviewers that the rights and welfare of individuals who may be asked to participate in this study will be respected, and that the research will be conducted in a manner consistent with the IRB requirements as outlined in section 45 CFR 46.

☒ The final versions of any printed recruitment, consent and assent documents bearing the IRB approval stamp are attached to this letter. These are the versions that must be used during the study.

As Principal Investigator, it is your responsibility to do the following:

1. Conduct this study exactly as it has been approved. Any modifications to the research protocol must be submitted with the appropriate signatures for IRB approval.
2. Submit a request for continuation if the study extends beyond the approval period of one calendar year. This continuation must receive IRB review and approval before the research can continue.
3. Report any adverse events to the IRB Chair promptly. Adverse events are those which are unanticipated and impact the subjects during the course of this research; and
4. Notify the IRB office in writing when your research project is complete.

Please note that approved protocols are subject to monitoring by the IRB and that the IRB office has the authority to inspect research records associated with this protocol at any time. If you have questions about the IRB procedures or need any assistance from the Board, please contact Beth McTernan in 219 Cordell North (phone: 405-744-5700, beth.mcternan@okstate.edu).

Sincerely,

Shelia Kennison, Chair
Institutional Review Board

APPENDIX B

APPROVED INFORMED CONSENT FORM

INFORMED CONSENT DOCUMENT
Robert G. Wood

Project Title:

A security risk analysis of the data communications network proposed in the NextGen air traffic control system

Investigator:

Robert G. Wood, candidate for Doctor of Applied Education
MS - University of Texas, Information Technology – Infrastructure Assurance
BS - Southern Nazarene University, Network Management
AT - Kansas State University, Computer Science

Purpose:

The purpose of this qualitative study is to conduct detailed personal interviews with aviation industry resources from one to four participants at each of five to ten purpose selected aviation organizations. The purpose of the interviews is to determine perceptions of aviation industry organizations regarding the active network design of the NextGen air traffic control system, determine potential gaps between the design and computer industry security standards, and obtain recommendations for future enhancements to the NextGen network design.

The implementation of the NextGen air traffic control system will induce major shifts in the methods used to separate and direct aircraft, and an ever-increasing need for security within the system is imperative in a post-911 world. Information, analysis, and threat identification will be essential in this rapidly changing environment.

Procedures:

As an active participant in this research study, you will be asked a series of predetermined set of questions. You will be recorded using a personal digital voice recording system. The interviews will be conducted at your place of business with the purpose of providing a comfortable and non-threatening environment. The interview is anticipated to take no longer than two hours and is expected to be conducted during one encounter.

Although direct quotes will be used in the study, all data results will be reported as group findings only and will not include information that will identify the interviewee. Neither interviewee names nor company names will be associated with the study.

The interview method will be utilized to determine what government and industry aviation organizations think are the critical security requirements needed for the active network within the NextGen air traffic control system. These questions were developed in order to compile a list of government and aviation industry security needs. Topics include, but are not limited to: 1) what are the perceptions of aviation organizations regarding the security needs of the NextGen air traffic control system?; 2) what gaps exist in the current design of active network in the NextGen air traffic control system between what is needed by the aviation industry and current accepted network security standards such as FISMA and NIST 800-42?; 3) What specific modifications are recommended by the aviation industry to eliminate this gap?; 4) How can industry, education, and government work together to address the security needs of the industry and successfully feed the pipeline of intellectual capital? (NextGen program enhancements, partnerships, internships, etc.)

A small sample of one to four participants at each of five to ten aviation organizations from government and industry were interviewed and asked a specific set of questions. This method of gathering data was appropriate due to the nature of the study and the precise documentation required for identifying industry security requirements.

You were selected as one of the participants due to your role within the identified aviation organization population and your position within your organization. The selection of all the participants was based on obtaining information related to the needs of each identified aviation organization. This sample was purposively chosen because it was believed to be a rich source of data for identifying security requirements for the NextGen air traffic control system.

Risks of Participation:

There are no known risks associated with this project which are greater than those ordinarily encountered in daily life.

Benefits:

This study will provide information to academia, the public sector, industry, and aviation users which could result in system safety and security improvements prior to full implementation of the NextGen air traffic control system in 2025. The study may also be used to assist in developing new curriculums to address the expanding role of computer and network technologies in aviation. As more and more computer systems find their way into the cockpit, the convergence of technology and aviation will provide additional avenues for Oklahoma businesses and professionals to grow through advanced education

Confidentiality:

The interviewees will be recorded in English using a personal digital voice recording system. The records of this study will be kept private. All data results will be reported in English as group findings only and will not include information that will identify the interviewee. Neither participant names nor organization names will be associated with the study. Data will be stored in secured computer files accessible only to the investigator and assistants. Audio recordings will also be stored in secure computer files and precautions will be observed to maintain confidentiality when airing the information. Research records will be stored in an encrypted manner on a secure server located at the researcher's residence and only researchers and individuals responsible for research oversight will have access to the records. To maximize both fidelity and security, transcription will be managed directly by the researcher. The data obtained from this research will be kept for a maximum of one year. After one year has lapsed, the data will be permanently destroyed. This signed consent document will be collected and stored separately to maintain confidentiality.

It is possible that the consent process and data collection will be observed by research oversight staff responsible for safeguarding the rights and well being of people who participate in research. The OSU IRB has the Authority to inspect consent records and data files to assure compliance with approved procedures.

Compensation:

There will be no compensation given for participation in this research project.

Contacts:

Primary Investigator:
Robert G. Wood
317 S. Chardon Drive
Mustang, OK 73064-1321
robert.g.wood@okstate.edu

Advisor:
Dr. Mary Kutz
Oklahoma State University
319 Willard Hall
Stillwater, OK 74048
mary.kutz@okstate.edu

If you have questions about your rights as a research volunteer, you may contact Dr. Shelia Kennison, IRB Chair, 219 Cordell North, Stillwater, OK 74078, 405-744-1676 or irb@okstate.edu.

Participant Rights:

Participation in this research project is voluntary and participants can discontinue the research activity at any time without reprisal or penalty. There will be no risk to any participants due to withdrawal from research project.

Signatures:

I have read and fully understand the consent form. I sign it freely and voluntarily. A copy of this form has been given to me.

_____ _____

Signature of Participant Date

I certify that I have personally explained this document before requesting that the participant schedule an interview.

_____ _____

Signature of Researcher Date

APPENDIX C

INTERVIEW QUESTION GUIDE

QUESTIONNAIRE: NEXTGEN ADS-B NETWORK SECURITY
Robert G. Wood

Before we begin, let me first ask you a few formal questions regarding the organization you're representing and yourself.

Section A: Formal data about the organization

[Interviewer should fill in this page at the beginning of the interview.]

Q1. Name of the organization: _____

Q2. Name and position of the interviewed person: _____

Thank you for this formal data Now, let's turn to the most interesting and informative questions.

Section B. Main Questionnaire

The Federal Information Security Management Act of 2002 defines three security objectives for information and information systems as:

CONFIDENTIALITY
"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY
"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY
"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Q3. Does the ADS-B portion of the NextGen active network provide confidentiality by preventing the unauthorized disclosure of information?

Q4. Is there a reason to limit confidentiality within the ADS-B network?

Q5. Is there information within ADS-B that should not (or must not) remain confidential? If so, why or why not?

Q6. **Does the ADS-B portion of the NextGen active network guard against improper modification or destruction of information?**

Q7. **What methods are utilized to insure data integrity?**

Q8. **How are ADS-B aircraft transmissions authenticated?**

Q9. **How are ADS-B ground station transmissions authenticated?**

Q10. **How are ADS-B satellite transmissions authenticated? Is authentication required?**

Q11. **Does the ADS-B portion of the NextGen active network insure availability by preventing disruptions from intentional or unintentional interference?**

Q12. **Is it critical for the ADS-B portion of the NextGen active network to ensure the timely and reliable access to navigation and control information?**

Q13. **What are your perceptions regarding the security needs of the ADS-B portion of the NextGen air traffic control system?**

Q14. **What gaps exist in the current design of the ADS-B portion of the NextGen air traffic control system between what is needed by the aviation industry and current accepted computer network security standards such as FISMA?**

Q15. **What specific modifications could you recommend to eliminate this gap?**

Q16. **What is the financial impact to your organization in moving to ADS-B and NextGen?**

Q17. **How can industry, education, and government work together to address the security needs of the industry and successfully feed the pipeline of intellectual capital?**

Q18. **That's all questions I have. Thank you very much for your cooperation and honest answers. Is there anything else you would like to add?**

Section C. Interview Information Sheet

[To be filled outafter the completion of the interview.]

Q19. The interview took place at:
___ / ____ (month) / 2008

Q20. Starting time:
___ : ___

Q21. Finish time:
___ : ___

Q22. Duration of the interview:
____.____ hours

Q23. The interview was conducted in (circle one)
- the organization's office
- at a conference or workshop
- other place (specify below)

Q24. The audio data file is saved as:
_____.wmv

Q25. Special circumstances of the interview:

APPENDIX D

SAMPLE ORGANIZATION APPROVAL LETTER

[redacted] <--- Corporate Letterhead

January 15, 2009

Mr. Robert G. Wood
Doctoral Candidate
Oklahoma State University

Dear Mr. Wood:

This letter documents my approval for you to interview personnel working with this organization while conducting research as part of a study entitled "*A security risk analysis of the data communications network proposed in the NextGen air traffic control system* ."

Please contact me at [redacted] if you require further assistance.

Sincerely,

[redacted] <---Authorized Signature

VITA

Robert G. Wood

Candidate for the Degree of

Doctor of Education

Dissertation: A SECURITY RISK ANALYSIS OF THE DATA COMMUNICATIONS NETWORK PROPOSED IN THE NEXTGEN AIR TRAFFIC CONTROL SYSTEM

Major Field: Applied Educational Studies, Aviation & Space Science Specialization

Biographical:

Personal Data: Born Bartlesville, Oklahoma, May 2, 1958.

Education: Received Associate of Technology degree in Computer Science from Kansas State University, May 1980; received a Bachelor of Science degree in Network Management from Southern Nazarene University, May 2002; received a Master of Science degree in Information Technology with Infrastructure Assurance concentration from the University of Texas at San Antonio, May 2006; completed requirements for a Doctor of Education degree in Applied Educational Studies, Aviation and Space, from Oklahoma State University, May 2009.

Professional Experience: Vice President & Program Director, L-3 Communications 2005 to present; Senior Vice President, Apptis Inc. 2002 to 2005; Vice President & CIO, Advancia Corp. 1999 to 2002; Vice President, BTG Inc. 1985 to 1999; Sr. Systems Analyst, Control Data Corporation 1980 to 1985.

Teaching Experience: Adjunct Professor at Southern Nazarene University, Bethany, Oklahoma, Network Management, 2002 to present

Professional Certifications: Certified Information Systems Security Professional; Certified Secure Software Lifecycle Professional; Program Management Professional (PgMP); Project Management Professional (PMP); Microsoft Certified Systems Engineer, Systems Administrator, Database Administrator, Solution Developer, & Trainer

Name: Robert G. Wood Date of Degree: May, 2009

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: A SECURITY RISK ANALYSIS OF THE DATA COMMUNICATIONS NETWORK PROPOSED IN THE NEXTGEN AIR TRAFFIC CONTROL SYSTEM

Pages in Study: 107 Candidate for the Degree of Doctor of Education

Major Field: Applied Educational Studies (Aviation & Space Science Specialization)

Scope and Method of Study: Aerospace Security Stakeholder Qualitative Interviews.

Interests internal and external to the United States could wreak havoc by manipulating, impairing, or data mining the digital information being exchanged by aircraft and controllers in the proposed NextGen air traffic control system.

The purpose of this study is the analyze potential security risks imposed by implementing the active network technologies utilized by ADS-B in NextGen, and more specifically the air-to-air, air-to-ground, and satellite-to-air links used. The purpose of this study was to provide a risk analysis of the NextGen active network compared to industry standards and best practices for information systems security. Data obtained through interviews was used to determine the effective security categorization and provide a risk analysis of the ADS-B portion of the proposed NextGen active network.

Findings and Conclusions:

Based on this research, there are both significant similarities and differences between the NextGen Active Network and industry standard computer networks. Both the ADS-B and computer networks operate in a wireless environment. Both are designed to move information between local devices, though the ADS-B devices may cover 200-300 miles at altitude where the computer networks are designed to cover a range of 200-300 feet. Both have methods of insuring a high level of data integrity using FEC, CRC, 24-bit parity, or MAC codes. It is at this point that the similarities diverge, as the missions of the two networks are markedly different. Specific conclusions and recommendations cover the differences between the designed mission requirements of NextGen and existing computer security standards focusing on the security objectives within the Federal Information Security Management Act of 2002 and other pertinent government standards and industry best practices.

ADVISER'S APPROVAL: Dr. Mary N. Kutz