EMBRY-RIDDLE
Aeronautical University
SCHOLARLY COMMONS

Publications

Summer 6-2-2016

Aircraft Cyber Security and Information Exchange Safety Analysis for Department of Commerce

Timothy B. Holt
Embry-Riddle Aeronautical University, holtt@erau.edu

Mohammad Moallemi
Embry-Riddle Aeronautical University

Linda Weiland
Embry-Riddle Aeronautical University

Matt Earnhardt
Embry-Riddle Aeronautical University

Sonya McMullen
Embry-Riddle Aeronautical University

Follow this and additional works at: https://commons.erau.edu/publication

 Part of the Aviation Safety and Security Commons, and the Management and Operations Commons

Scholarly Commons Citation

Holt, T.B., Moallemi, M., Weiland, L., Earnhardt, M., & McMullen, S. Department of Commerce. (2016). Aircraft cyber security and information exchange safety analysis for the department of commerce.

This Report is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Publications by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

Aircraft Cyber Security and Information Exchange Safety Analysis for Department of Commerce

Timothy Holt, Ph.D.
College of Business, Worldwide
Embry-Riddle Aeronautical University

Mohammad Moallemi, Ph.D.
Next Generation Applied Research (NEAR) Lab.
Embry-Riddle Aeronautical University

Linda Weiland
College of Aeronautics, Worldwide
Embry-Riddle Aeronautical University

Matt Earnhardt, Ph.D.
College of Business, Worldwide
Embry-Riddle Aeronautical University

Sonya McMullen, Ph.D.
College of Aeronautics, Worldwide
Embry-Riddle Aeronautical University

Summary

The Federal Aviation Administration's (FAA) Next Generation Air Transportation (NextGen) program is a long-term modernization and transformation of the current National Airspace System (NAS) into a more effective and coordinated decision-making system. NextGen provides a more reliable, secure, and dependable aviation capability for both users and operators ensuring more capacity, throughput, and safety. This research delineates a high-level Safety Risk Assessment (SRA) related to NextGen technologies, specifically Aircraft Communications Addressing and Reporting System (ACARS) as well as Aircraft Access to System Wide Information Management (SWIM) network (AAtS). Other communication mediums such as Mode-S or ADS-B transponder are also data exchange and broadcast capabilities in the aircraft can also be prone to lower level safety risks primarily because of an inability to ensure information security.

Scope

In the context of information security/protection, a threat agent (threat source) is an individual, instance, or component that poses danger to assets which need to be protected. Figure 1 depicts typical ACARS system components: (a) Multi Communication Display Unit (MCDU), (b) Flight Management System (FMS), (c) Autopilot, the Flight Deck Interval Management (FIM) Equipment, (d) Communication Management Unit (CMU), and (e) datalink. Details such as various Instrument Flight Rules (IFR) points, flight plan, and navigation points are programmed into FMS, and the aircraft essentially follows these commands via the autopilot. Aside from these components, AAtS aircraft assets typically include Electronic Flight Bag (EFB) and onboard internet router and modem.

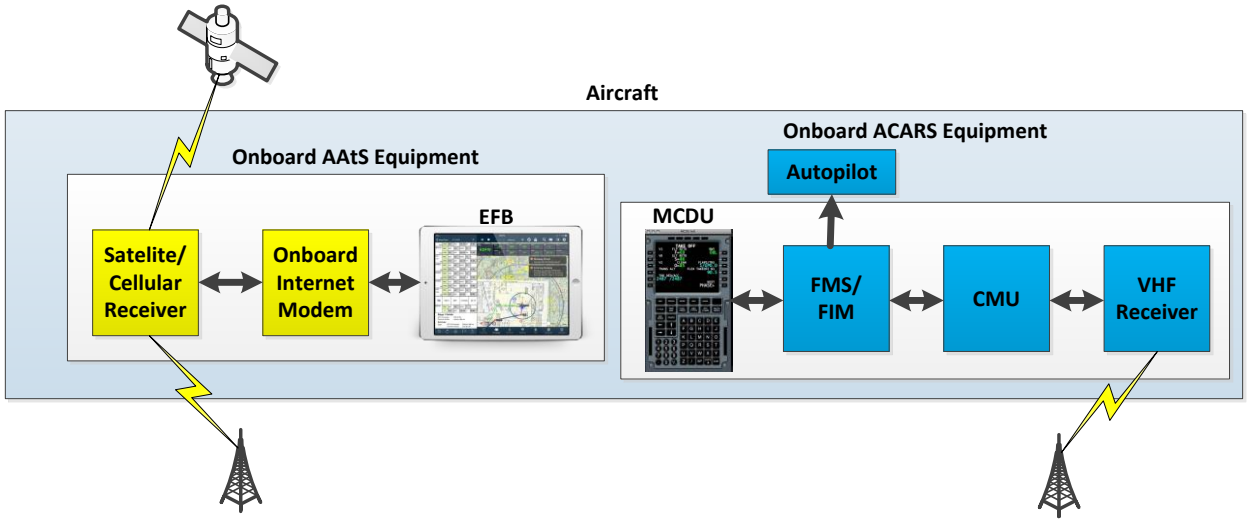

Figure 1. Major ACARS and AAtS Onboard Components

Federal Information Processing Standards (FIPS) defines a threat as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." Attack vectors are routers or means by which a threat agent can influence assets or legitimate access to assets.

Based on this definition we will classify threat actions as:

- Access: simple unauthorized access (e.g. unauthorized access to FMS, or EFB)
- Misuse: unauthorized use of assets (e.g. unauthorized use of CMU, or onboard internet router)
- Disclosure: unauthorized and illicit disclosure of information (e.g. publishing FMS or EFB credentials or confidential data)
- Modification: making unauthorized changes to an asset (e.g. modifying the route submitted via ACARS, or modify weather data, or Air Traffic Control (ATC) Winds or Air Operations Center (AOC) Winds data)
- Denial of access: blocking legitimate users from accessing assets (e.g. consuming bandwidth and/or blocking MCDU logon access to Air Route Traffic Control Centers also known as ARTCC stations)

Within scope of the NextGen program is integration of Trajectory-Based Operations (TBO) with ACARS and AAtS systems. Use of air/ground Aeronautical Telecommunication Network Baseline 2 (ATN-B2) data communications; flight object; integration of Air Traffic Management (ATM); Flight Operations Center (FOC); and aircraft trajectory communication systems for advanced trajectory exchange in ATM capitalizes the role of SRA research on ACARS. Proposed new capabilities such as Dynamic-Required Navigational Performance (D-RNP), Advanced flight Interval Management (A-IM), and ATC winds are examples of the exchange of mission critical data over ACRS. In addition, A-IM Concepts of Operations (ConOP) developed by the Radio Technical Commission for Aeronautics, or RTCA, and provided by Special Committees SC-186 and SC-214 released on March 27, 2014, and subsequent releases advocate for incorporating TBO communication via ACARS and directly loading it into FMS/FIM equipment. Flight deck Data Communication equipment will provide a "direct load" capability that will allow loading Advanced Information Management (IM) application clearance information, including Target IFPI, directly into the FIM equipment. These features, while they increase automation and agility of aircraft systems, pose significant security risks to onboard flight control equipment, when proper policies, equipment, and encryption of data is not used.

On the other hand, AAtS Implementation guidance released March 1, 2013, states that "Information is intended to support but not directly change the trajectory of the aircraft. Examples of non-trajectory affecting information include wind, temperature and turbulence information for presentation to the pilot or upload into the flight management function (FMF)." Although AAtS is not currently planned to carry direct trajectory related data, there are non-mission critical data transferred via this medium that directly affect situational-awareness and subsequently decision making of the flight crew.

Threat Agent Identification and Assessment Methodology

There are certain challenges in securely delivering the ATC/AOC clearances/instructions via ACARS to the MCDU and vice-versa that must be addressed and overcome. In this research, we are identifying sets of potential and imminent threats including threat vectors regarding information transfer within ACARS and AAtS framework. The risk factor for each threat can be analyzed and determined based on the categorization proposed in Document DO-178C software development standard. Software level determination and failure-condition categorization processes need to be followed to assess threats and their severity. Potential measures to address threats and mitigation strategies are also needed. In the following subsections, we discuss overarching threat categories that needs to be further investigated for ACARS and AAtS. It must be mentioned that these are not all the threat categories and more in-depth research and collaboration with stakeholders (i.e. aircraft avionics manufactures, datalink service providers, data management service providers …) will shape the ultimate SRA assessment.

Denial of Service to ACARS/AAtS Resources

Denial of Service (DoS) is the mechanism in which an attacker attempts to saturate network resources to the degree that computing components of the network are no longer able to process requests due to overload conditions in the network. This will cause onboard MCDU, EFB, CMU, router, modem, and other components to get out of reach and halt services produced by them. Currently, ACARS communication protocols such as Controller Pilot Datalink Communication (CPDLC), Aeronautical Radio Inc. (ARINC 702), and ADS-C are not encrypted and are operating based on a trusted network. All current aviation communications are unauthenticated and unencrypted whether sent by aircraft or ground ATC systems.

ACARS/AAtS Datalink Mapping

In assessing vulnerability and security of a network, any loose node that does not follow security standards can be a foothold for attackers to get into more sensitive parts of networks and databases. Network mapping is one strategy used by attackers to locate vulnerable nodes in a network and breach them. By using Open Source Intelligence (OSINT) techniques and tools, it is possible to map ACARS/AAtS networks and aircraft components and services without actually sending any packets (or just a few standard requests). An unauthenticated user of ACARS (due to lack of proper authentication mechanisms) might be able to conduct reconnaissance on datalink provider's network to map networks along with fingerprinting aircraft CMUs, MCDUs, EFBs, etc.

ACARS/AAtS Data Encryption

Network communication certificates such as Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols protect network users in two-way communications. The goal is to maintain privacy of data by establishing encryption on data being communicated as well as authenticating identity of senders and receivers. Due to lack of encryption in ACARS air to ground communications as well as the onboard ARINC 429 data-bus, a potential attacker can easily sniff data and possibly modify/omit messages, navigational databases on FMSs, or autopilot control loops. As it was mentioned earlier, direct loading of ATC route and instructions into FMSs is a future goal of the NextGen program, posing a potential threat to aircraft's safety. On the other hand, limited encryption is used in AAtS that might allow attack on the certificate authority of EFB using rouge certificates.

Man-In-The-Middle Attack to ACARS/AAtS Datalink

Man-In-The-Middle (MITM) refers to an attacker's effort in relaying and possibly altering data transfer within network components. The attacker intercepts all communication between two victims who believe they are communicating directly. Using Software-Defined Radio (SDR), software, and ACARS communication standards (e.g. CPDLC, ATN-B1/B2) available on the Internet, a transmitter/receiver unit can be built and used to spoof an ATC ground station or another aircraft. Attackers can rouge FMS impersonating the real FMS to conduct MITM attack on ACARS data traffic to tATC/AOC, due to lack of a secured authentication mechanism in ACARS.

Human Factors

Akopyan and Yelakov (2009), called cybercrimes a global disaster that needs to be corrected, in discussing cyber security, it is important to consider human factors associated with cyber security. As stated by Bowen and Stolfo (2012), computer security is not just about technology but those people that use systems and how their behaviors can lead to exploitation. Widdowson and Goodliff (2015), indicated that the human element contributed to over 95% of all security incidents. In considering human factors associated with cyber security, the CHEAT model could be used, of which 57 human factors derive the model in five categories: (a) technology, (b) people, (c) organization, (d) history, and (e) environment. This model allows for a proactive assessment of vulnerability and root causes of human-related events. The model works by not only identifying root causes but then identifying solutions. In considering exploitation of the human side, solid metrics will be needed to assess vulnerabilities before deployment of resources. Carr (2016), advocated a cyber-security strategy that focuses on both public and private partnerships in mitigation of cyber security threats. Applying this approach to the human factors side, risk assessment and training is critical before corporations should invest in overseas markets. White, Hewitt, and Kruck (2013) indicated that, in order to reduce human factors, cyber security needs to be a core component of the organization.

Conclusions

To properly pinpoint and mitigate these potential risks, an engineering team should refine the identified threats and initial risk assessment. Failure condition categorization based on DO-178C standards for large transport category aircraft based on established advisory material for system safety assessment processes need to be carried out. Once threat mitigation strategies are developed, a comprehensive test plan for the two mentioned SRAs, and any additional SRAs proposed by FAA with verification of mitigation strategies need to be developed and tested. These tests are expected to result in both real and national information security threat mitigation strategies, network architectures for assured security and quality of service, and a better understanding of limitations/capabilities of ACARS and AAtS. A set of authentication and data encryption techniques along with their pros and cons as well as their suitability must be identified and implemented on these networks. In addition, a set of desired security measures including those that need to be implemented on ACARS and AAtS resources, servers, routers, modems, and computing systems need to be established and standardized as recommendations and mitigation strategies.

Examining Marketing opportunities for Cyber Security Companies to meet the Threats of Cyber Security in Aviation

Air Traffic Management (ATM) is complex and further complexity comes from Cyber Security threats. Cyber-attacks in ATM are of concern in the aviation industry and there have been market studies around both threats to and business opportunities for companies that are able to find vulnerabilities and offer solutions. Organizations in the aviation industry have started to hold Cyber-Security summits to better understand a variety of situations and look to solutions.

In aviation, there is heavy reliance on computers to control and fly complex aircraft, and for coordination of all ATM movements. Some questions arise that may result in the air traveling public afraid to fly. Can terrorist take over airplanes? What can terrorist do to ATM or aircraft? Damage that can be done onboard to Information Technology (IT) systems could be devastating to safety of flight and to the aviation industry. Though ADS-B is designed to move aircraft safely and efficiently these systems are an "open architecture," there is risk in use of it in highly dense areas or air traffic so the risk vs the strengths are crucial to aviation.-I'm not comfortable making these changes, I do not want to alter the intent. However, I do believe this section needs revision.

*The State of Security from Tripwire, Lane Thames in June of 2015 wrote "*Did The Aviation Industry Fail Cybersecurity 101* and it he discussed the infamous tweet that a passenger on a United Airlines was removed for and investigated for a cyber-attack. In the article he wrote about the key players, what their problems are, where they failed, poor security and poor incident response, all, which should be troubling to the public. Recommend this be revised and the in text citation Thames be used in accordance with APA recommendations.

Cyber Security measures need to identify vulnerabilities, the risks, and stakeholders, along with solutions. The research firm, Visiongain, conducted a report that concurs with others and agrees that it should be done with regions in mind, and the areas would be North America, Europe, Asia-Pacific, Middle East, South America, and Africa. The report also identified and provided profiles on companies that were believed to be leading the market. The details included 16 leading tech companies and more than 120 companies that are operating in the aviation cyber security market. The focus of this paper is on ATM opportunities, but one must realize opportunities overlap in the aviation industry and the entire market should be looked at in total.

In December of 2015, there was an Aviation cyber-security think tank in Washington, DC., it reviewed the vulnerable points, which include WiFi, Inflight entertainment, On board mobile and pilot devices along with avionics, avionics' being the way of the future for communication with ATM. The National Cybersecurity Center for Excellence (NCCoE) and the National Institute of Standards and Technology (NIST) as part of the U.S Department of Commerce hosted the event. The aviation think tank discussed how in June of 2015, hackers were able to steal data on flight manifests, corporate data, seat numbers departures and other items. In their conference prelude, they reminded people that United American Sabre Polish carrier LOT and others have been victims of cyber-attacks. Workshops included undertaking the complexity of ATM and managing the vulnerability points and what does Air Traffic Control (ATC) future hold in technology improvements. -I recommend that the results or findings of the think tank should be reported and then cited per the APA.

The State of Security from Tripwire, Lane Thames in June of 2015 wrote "*Did The Aviation Industry Fail Cybersecurity 101* and it he discussed the infamous tweet that a passenger on a United Airlines was removed for and investigated for a cyber-attack. In the article he wrote about the key players, what their problems are, where they failed, poor security and poor incident response, all, which should be troubling to the public. Cyber security measures need to identify vulnerabilities, the risks, and stakeholders, along with solutions. –this was previously used, see * above.

The Air Traffic Control Association (ATCA) held a cyber – security event in January 2016, which was after the November 2015 Aviation Cyber Conference think tank. ATCA produced a white

paper that discussed how hardening they systems and having a strategic plan could help prevent breaches in ATM.-here again, I recommend that pertinent facts from the think tank be discussed and then cite the cyber-security event; proceedings, conference, etc.

Organizations such as; Cyber Security Service and Solution Providers, Airlines (planes) and Airports (airport facilities to include Air Traffic Control) have identified the key stakeholders. They state that there is a market by component solution and service, by deployments On – Cloud and On – Ground and in agreement with Civil Air Navigation Services Organization (CANSO) and International Civil Aviation Organization (ICAO) on Identifying and solving the situation by Regions.

Visiongain's Senior Aviation Analyst and Consultant and author of "*Aviation Cyber Security Market Forecast 2015-2025"* , commented in Visiongain in March of 2015, "The threat of an aviation industry cyber-attack is real" (Para 1 2015). He also noted that most of the attacks have been with criminal or terrorist intent. He also provided in his market analysis the four submarkets, which are Airline/Aircraft systems, Airports systems, Computer reservations systems/ Global Distribution System (CRS/GDS), and Air Traffic Management systems in Cyber-security

PRNews wire did an article on "*Aviation & Defense Cyber Security Market By Component, by Deployment &by region –Rise in cyber-attacks is a major factor increasing the procurement of aviation Cyber Security Solutions and Services".* They stated," The global aviation cyber security market is expected to grow from USD 39.59 billion in 2015 to USD 61.85 billion by 2020, at a Compound Annual Growth Rate (CAGR) of 9.34% from 2015 to 2020. Factors influencing the growth of this market include rise in malicious cyber-attack & cybercrimes and increase in digitization of operations in the aerospace and defense sector" (Para 1 2016).

Looking for market opportunities in North and South America show there is a significant need and a market for cyber-security to protect avionics and other ATM equipment that would be able to benefit with collaboration, partnerships and joint ventures. The segments also are divided in solution type and security type. The increasing need for both solution type and security type solutions is creating large opportunities for the market. Some of the areas in the market that are growing include; identification access management, firewalls, antivirus and anti-malware, disaster recovery, data loss protection, and threat management along with risk assessment and education training.

Markets and Markets, for state there are two types of cyber-security solutions called on-cloud and on premise. The on-cloud is a network based solution, and on-ground would be hard drives, and local equipment solutions. There are benefits and risks to both so a hybrid solution would be the best way to proceed. The market needs a set of technologies that have solutions and tools for the user.

The cyber-security market is looking at consulting, design and integration, risk and threat assessment, managed security services and train and education. There are types of security and equipment security that have a growing market too. The data shows that industry experts are involved. These include International Business Machines Corporation (IBM), Honeywell International, INC., CISCO systems Inc., Raytheon, BAE, Lockheed Martin and Northrup Grumman Corporation to name some of them.

These companies have worked with the Aircraft Communications Addressing and Reporting Systems (ACARS), the components include the MCDU, FMS, FIM, CMU, and Datalink. Linkedin Pulse

did a recent article that South America is poised to have a large CAGR over the next few years and some countries have adopted cyber-crime laws, which also enhances market opportunities for companies that are able to find the solutions for equipment that is used in more than one continent.

Dublin –Business reviewed a Research and Markets report that showed that there is a market for a cyber-security framework in the aviation industry and the trends in the market place is growing. They also pointed out that secure functioning of these aviation systems and safety from possible attacks is a collective responsibility. The stakeholders according to the article include governments, airlines and airports. They also point out the opportunity for business for the above companies. A Secure World Expo also predicted growth for the same countries and companies.

Research of the companies and there recruitment/involvement in cyber-security shows similar statistics. IBM has advertised for employees in cyber-security and has also produced white papers stating their competency in the field and willingness to solve data breach risks. IBM in 2010 did a press release on their work with the Federal Aviation Administration (FAA) in cyber-security. They have experts designing and building a prototype security system for the FAA complex networks.

Honeywell has a link on their webpage that discusses Cybersecurity, Biometric and Physical Security capabilities they have and are needed for companies to protect the enterprise, employees and customers. CISCO connected aviation has also addressed their capabilities is solving some of the aviation cyber-security risks. Recently they gave a press release on their work at Athens International Airport. Raytheon has a cyber-security operations department and is actively recruiting employees for cyber-security positions. Lockheed Martin and Northrup Grumman also have departments. It appears most major companies in Aviation cyber–security know there is a need for better security in aviation, have been doing the research, and they are offering solutions to the other stake holders. They are also offering employment opportunities as they too predict the need in the market.

References

Advanced Interval Management (Focus: RTCA Special Committee 214 Tasking) Preliminary Concept of Operations, version 1.0, FAA, March 27, 2014

Advanced Interval Management (A-IM) Arrival, Approach, Departure, and Defined Interval Operational Service Description (Final Draft), Baseline Document: ASPA-FIM SPR ED-195/DO-328 REV A, DRAFT V1.05, Prepared By RTCA SC-186 WG4 / WG51

Aircraft Access to SWIM Implementation Guidance Document, Version 2.0, 1 March 2013

ARINC Characteristic 758-2 Communications Management Unit (CMU) Mark 2. ARINC. July 2005

Aviation & Defense Cyber Security Market By Component, by Deployment &by region –Rise in cyber-attacks is a major factor increasing the procurement of aviation Cyber Security Solutions and Services (2016) retrieved from http://www.prnewswire.com/news-releases/aviation--defense-cyber-security-market-by-component-by-deployment--by-region---forecast-to-2020-300205435.html

Boeing (2013) *developing a framework to Improve Critical Infrastructure Cybersecurity* retrieved from http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160208_Boeing.pdf

Business Wire (2015) *Research and Markets: Global Aviation CyberSecurity Market 2014-2018 with Boeing (Defence, Space, and security (BDS)), Harris, IBM, Intel (incl. McAfee Inc.) & Symantec Dominating* (2015) retrieved from http://www.businesswire.com/news/home/20150127006297/en/Research-Markets-Global-Aviation-Cyber-Security-Market

CSFI ATC (Air Traffic Control) Cyber Security Project, July 16, 2015, available at: http://www.csfi.us/pubdocs/?id=47, accessed May 2016

DO-178C Software Considerations in Airborne Systems and Equipment Certification, RTCA Committee: SC-205. December 13 2011

Dynamic Required Navigation Performance (Focus: RTCA Special Committee 214 Tasking) Preliminary Concept of Operations, version 1.0, FAA, March 27, 2014

Elias, B. (2015). *Protecting civil aviation from cyberattacks* retrieved from https://www.fas.org/sgp/crs/homesec/IN10296.pdf

FAA Needs to Address Weaknesses in Air Traffic Control Systems, United States Government Accountability Office Report to Congressional Requesters (Information Security). January 2015, available at: http://www.gao.gov/assets/670/668169.pdf, accessed May 2016

Furlani, C.M. (2009). *Minimum security requirements for federal information and information systems.* DIANE Publishing

Global Aviation Cyber Security Market to be Worth $1.B Bn in 2015 According to New Visiongain report (n.d.) retrieved from https://www.visiongain.com/Press_Release/787/Global-aviation-cyber-security-market-to-be-worth-1-8BN-in-2015-According-to-new-Visiongain-report https://www-

IBM to design and Build Advanced Cyber Security Analytics System for the U.S. Federal Aviation Administration (2010) Retrieved from www.03.ibm.com/press/us/en/pressrelease/29782.wss#release

Interoperability Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 Interop Standard), RTCA DO-351 REVA, volumes 1 and 2, RTCA SC-214, April 4, 2016

Interoperability Requirements Standard for Baseline 2 ATS Data Communications, FANS 1/A Accommodation (FANS 1/A - Baseline 2 Interop Standard), RTCA DO-352 REV A, RTCA SC-214, April 4, 2016

Interoperability Requirements Standard for Baseline 2 ATS Data Communications, ATN Baseline 1 Accommodation (ATN Baseline 1 - Baseline 2 Interop Standard), RTCA DO-353 REVA, version 1A, RTCA SC-214, April 4, 2016

NextGen Implementation Plan Document, June 2013

Safety and Performance Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard), RTCA DO-350, REVA, volumes 1 and 2, RTCA SC-214, April 4, 2016

Shirey, R.W. (2016*). Internet security glossary, 2000*. Available at: http://tools.ietf.org/html/rfc2828

Thames, Lane (2015) *Did the Aviation Industry Fail Cybersecurity 101* retrieved from http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-aviation-industry-did-they-fail-cybersecurity-101/

White, Garry L, CCP,C.I.S.S.P., PhD., Hewitt, B., PhD., & Kruck, S. E., P. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education, 24*(1), 11-16. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1438693461?accountid=27203

Williams, James (n.d.) *National Airspace System Security Cyber Architecture* retrieved from https://www.mitre.org/publications/technical-papers/national-airspace-system-security-cyber-architecture