CONNECTED AIRCRAFT: CYBER-SAFETY RISKS, INSIDER THREAT, AND MANAGEMENT APPROACHES

Abstract

The past several years has witnessed significant growth in Internet Protocol (IP)-based wireless connections between airborne aircraft, satellites, and terrestrial information systems, a phenomenon some have termed The Connected Aircraft (Bellamy, 2014). Far eclipsing passenger high-speed Internet service, this movement is integrating thousands of embedded automated sensors connected to safety-critical systems, such as engines, flight controls, cockpit displays, and life support systems into the on-line infrastructure. Airborne sensors continuously send data packets to worldwide airframe, engine, and avionics manufacturers, airline control centers, and third-party suppliers (Orjih, 2006). The tremendous growth in the Internet of Things (IoT), small, low-power, programmable, Internet-connected, smart devices, has accelerated the Connected Aircraft transformation (Lueth, 2014). In short, winged local area networks are expanding the Internet to 30,000 feet. However, connecting aircraft to the Internet is also exposing safety-critical airborne systems to serious cyber-physical safety risks, to which the traveling public is largely oblivious. This ignorance is likely to remain until, heaven forbid, a crash or other incident is directly linked to a successful cyberattack. This research paper will attempt to narrow this knowledge gap by shedding light on the growing cyber-physical safety risks of The Connected Aircraft. Next, it will discuss insider threat in the airline industry. It will also suggest risk management approaches, some already underway, to help reduce these emerging cyber-safety risks so that the promising operational, economic, and business benefits of movement can be realized without exposing the traveling public to undue safety risk.

1. Introduction

The combination of IoT devices and safety-critical airborne systems produces serious cyber-physical safety risks, to which the traveling public is largely oblivious. This state is likely to remain until, heaven forbid, an air disaster is directly linked to a successful cyberattack. This research paper will attempt to narrow the knowledge gap by shedding some light on the growing cyber-physical safety risks of The Connected Aircraft. Further, it will suggest risk management approaches, some already underway, to help reduce these emerging cyber-safety risks and enable the promising operational, economic, and business benefits of the Connected Aircraft phenomenon to be realized without exposing the traveling public to undue safety risk.

2. Background

Aviation electronics, a.k.a. avionics, have been with us since shortly after World War II, when the cathode ray tube, portable radar systems, and radio frequency- (RF) based communication & navigation systems began proliferating (Wikipedia, 2017). Significant advances were made with the introduction of integrated circuits, satellite communications, and electronic inertial navigation systems in the 1970s and 80s. The US Global Positioning System (GPS) was released for civilian use in the 1990s and was soon followed by several other constellations of Global Navigation Satellite Systems (GNSS) (Boyne & Crouch, 2016). In the late 1990s and early 2000s, the liquid crystal display (LCD), digital/software-driven cockpit control and display units (CDU), and integrated flight management systems (FMS) brought about the continuing era of the Glass Cockpit (Ashley & Attan, 2011).

Airplanes truly began to morph into cyber-physical systems with the introduction of Central Air Data Computers (CADC) driving all cockpit displays, full authority digital engine controls (FADEC) translating throttle movements to engine settings, digital fly-by-wire flight controls processing and communicating data from computers connected to physical cockpit controls to actuate external flight surfaces, and internal aircraft data busses to manage these growing airborne computer networks (Wikipedia, 2017). It wasn't until the about 2010 however, with the introduction of airborne Internet access (Martin, 2009) and the Federal Aviation Administration's (FAA) kickoff of the Next Generation Air Navigation System (NextGen) (FAA,

URI: https://hdl.handle.net/10125/59759
ISBN: 978-0-9981331-2-6

2018) that the RF-to-IP transformation markedly accelerated. The FAA's three major NextGen priorities are: (1) transforming nearly 30,000 terrestrial analog telecommunications circuits serving 5,000 facilities, into a 100% Internet-based communications network, (2) decommissioning ground-based radio navigation aid systems and relying totally on airborne GPS/GNSS navigation signals, and (3) replacing RF-based Air Traffic Control voice communications with textual packet-based data communications (like email/instant messaging) (FAA, 2016). Even GPS/GNSS satellite signals are being converted from analog to digital format (Brooks, 2015). With more and more ground, airborne, and space-based systems connecting via packet-based signals and the virtual explosion of embedded IP-based microprocessors and sensors joining the Internet, it is not difficult to understand that the Internet is expanding skyward.

3. Cyber-Safety Risks of Connected Aircraft

Dr. Edward Griffor in his *Handbook of System Safety and Security*, defines cyber-physical systems (CPS) as "systems that include both logical operations (such as control and feedback) and physical interactions, such as gathering information from the physical realm using sensors or taking an action or actuating that impacts the physical realm" (Griffor, 2016, p. 5).

Sampigethaya and Poovendran, point to the Boeing 787 as an example of an "e-enabled aircraft" in their Institute of Electronics and Electrical Engineers (IEEE) paper *Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport*, describing a combination of digital computing, storage, software, and networking that yields a "self-aware airborne node in a global information network" (Sampigethaya & Poovendran, 2013, p. 1836). The Connected Aircraft is another node in an emerging real-time network of airborne and ground service endpoints, sharing data on everything from flight parameters (airspeed, altitude, position, etc.), to engine temperatures, avionics status, and even brake wear (Bellamy, 2014).

However, by giving wings to the Internet, we have also elevated the many terrestrial cyber risks into the inherently dangerous realm of high-speed, high-altitude, all-weather transportation.

3.1. Integrated Modular Avionics

Cybersecurity is a new paradigm in aviation, we're going to have to protect the airborne and ground interfaces" John Craig, Chief Engineer, Cabin and Network Systems, Boeing Corp. (Bellamy, 2014).

Onboard avionics systems are being further transformed from an assortment of bus-federated modules, into a new Integrated Modular Avionics (IMA) architecture, employing multi-core, multi-processor computers for higher performance and throughput. This logical integration combines cabin environment, passenger entertainment, flight deck, flight control, system health, and other sub-networks/nodes (including passenger carry-on devices) into an integrated ecosystem approaching the complexity and sophistication of software-defined networks (SDN) (Sampigethaya & Poovendran, 2013). Figure 1 illustrates a high-level IMA architecture.

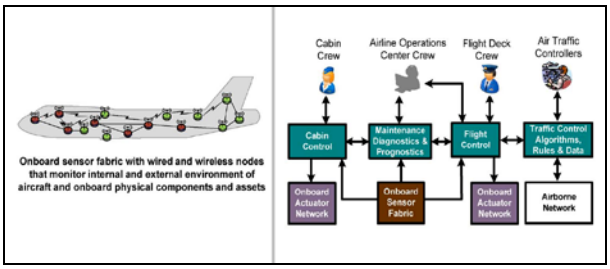

Figure 1. Onboard Integrated Modular Avionics Architecture

Boeing demonstrated the IMA business case on the 787 Dreamliner by replacing of over 100 separate onboard computers with one "Common Core System" (Ramsey, 2007, p. 1).

Though avionics software goes through a much more rigorous quality/reliability certification process than terrestrial programming, IMA networks, by adopting the architecture and supporting technology of terrestrial SDNs, inherit very similar vulnerabilities (Cyber Security Intelligence Ltd, 2015). These vulnerabilities include misconfigured firewalls, reconfigurable communications links, low-power wireless signals, weak (or no) cryptography, and loose traffic flow management layer permissions (Slavov, Migault, & Pourzandi, 2015).

Successful attacks on these types of systems have been theorized, attempted, and accomplished. Software security firm founder John McAfee firmly believes that aircraft can be hacked (McAfee, 2016). In 2015, the US General Accounting Office (GAO) reported that aircraft could theoretically be hacked and commandeered by hackers penetrating firewalls between passenger entertainment systems and cockpit avionics (GAO, 2015). Further, in 2015, aviation

security researcher Chris Roberts, told the FBI he had hacked into the onboard network of a United Airlines flight by penetrating the passenger entertainment system from his seat on the plane. Though his claims were disputed by others, he reportedly claimed to have "access[ed] in-flight networks about 15 times during various flights" (Zetter, 2015, p. 1) penetrating "the fuel balancing system and the thrust control system" (Zetter, 2015, p. 2).

Finally, in a widely publicized 2017 announcement, Robert Hickey, Program Manager of the US Department of Homeland Security (DHS) Cybersecurity Division, Science & Technology Directorate, announced that his team had successfully hacked into a parked DHS-owned Boeing 757 within two days after obtaining it, and with neither insider aid nor physical access (Biesecker, 2017) and (Paganini, 2017).

3.2. Full Authority Digital Engine Controls (FADEC)

Given that IMA architectures provide centralized access to other onboard digital systems, consider the cyber-safety risk of a hack into an airborne engine's FADEC, which Chris Roberts also claimed to have accomplished (Zetter, 2015). FADEC is a quite literal name in that this system has full authority over the engine it controls, i.e. no manual override (SCRIBD, 2018). Pilots and auto-throttle systems (also computer-driven) send messages to FADECs much like homeowners send desired room temperature messages to "smart home" controllers. From the hacker's point of view, he who controls the FADEC, controls the engine. From the pilot's perspective, he who controls the engines controls the aircraft. Fortunately, airliners are required to have two FADEC's per engine, but there is still just one IMA system.

3.3. Automatic Dependent Surveillance Broadcast (ADS-B)

A less obvious cyber-safety consideration involves a relatively new technology called Automatic Dependent Surveillance Broadcast (ADS-B). ADS-B is an efficient and effective system for networking airplanes and ground stations and is the FAA's next step beyond 1940's-era radar surveillance. Relying on GPS/GNSS signals for accurate and precise position and timing, ADS-B gives air traffic managers a clearer operational air picture, enabling them to let aircraft fly closer together. Pilots (and autopilots) use ADS-B for situational awareness, separation, and following other aircraft, as well as real-time graphical & textual weather information. Figure 2 shows the ADS-B system as part of NextGen.

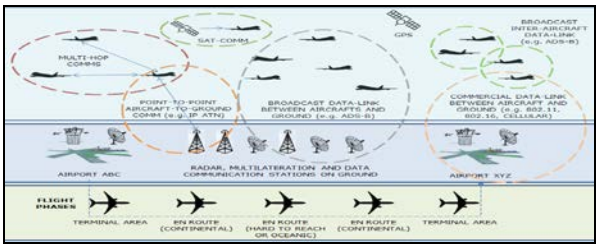

Figure 2. FAA NextGen with ADS-B

ADS-B employs an unencrypted and unauthenticated network communications protocol that presents several attack vectors to hackers (Sizemore, 2017). For example, a hacker could highjack the session of an airborne airliner and start sending packets indicating the aircraft is miles/thousands of feet away from its actual position. This could surprise and confuse air traffic managers, pilots, and autopilot systems, possibly causing an inflight collision. It could also cause the autopilot and Traffic Collision Avoidance System (TCAS) of an airplane immediately near the new false position to unexpectedly react with an abrupt avoidance maneuver (Storm, 2012). Since ADS-B is dependent on satellite signals, ADS-B ground stations, and onboard Wide Area Augmentation Systems (WAAS), these present three additional error injection pathways, i.e. threat vectors. GPS spoofing is probably the easiest attack in this context, because low-power satellite signals are easily overcome/jammed (Zimmerman, 2013). French researchers have also demonstrated that inserting "ghost aircraft" into the airborne ADS-B network could overwhelm the targeted geospatial area, causing denial of service (DoS) (Costin & Francillon, 2012).

3.4. Aircraft Health Management Systems

IoT-enabled real-time automated aircraft health management systems, monitoring engines, structures, avionics, and other safety-of-flight systems, present another broad cyber-safety risk area. IoT sensors are becoming more and more prevalent on aircraft, building automated wireless networks with continuous air-to-ground data transmission and collection nodes feeding huge databases. The Boeing Airplane Health Management (AHM) system, for example, ingests and analyzes terabytes of real-time

data from over 2000 aircraft from 53 worldwide airlines on fuel performance, engine oil consumption, and numerous flight parameters (e.g. airspeed, altitude, etc.) (Boeing Corp., 2013). Figure 3 shows Boeing 787 AHM data collection. Over 13,000 Rolls-Royce engines, flying on roughly 9,000 commercial flights/day, continuously send data messages through SITAOnAir's Aircom FlightMessenger service to Microsoft's Azure cloud platform for aggregation and analysis by the Cortana Intelligence Suite (Bellamy, III, 2017).

Figure 3. Boeing Airplane Health Management System on 787 Dreamliner

While hackers have many opportunities to frustrate health management systems, the more significant cyber-safety issues lie just ahead. Today's systems simply stream down and analyze real-time data to prognosticate and prepare for ground maintenance operations. The continuing quest for innovative cost efficiencies will likely soon drive on-wing/airborne maintenance. In other words, why wait until an engine, autopilot, cabin pressure, or other digital/digitally-controlled system arrives at an airport to fix a problem or perform routine inspection/maintenance when it can be done via a ground-to-air data-linked control of aircraft software, firmware, and hardware. If this coming evolution keeps the equipment onboard for even few more flights, or provides maintainers earlier troubleshooting data, this "fix-in-flight" approach will likely be irresistible. That miracle of networking technology however, will come the real possibility of global hackers penetrating, elevating privileges (if needed), and sending erroneous, harmful, or dangerous "fixes" to these systems while they cruise at 30,000 feet and 500 miles per hour, perhaps over open ocean (think Malaysian Air Flight 370). The challenge to hackers would be very enticing, making probability of attack significant. The impact could be life-threatening.

4. Insider Threat in the Air

4.1. Corpus Overview

As stated by Claycomb et al., a proven process exists for examining insider incidents and they involve several steps. One method is as follows: (1) Collect source data (e.g., documents, reports, etc.) on instances of insider crime. (2) Process case information using a repeatable and consistent process to store key information and events about the case. (3) Create chronological time-lines from case data. (4) Identify key events in the chronology of the attack. (5) Examine case chronologies to identify patterns of significant indicators of attack. (6) Compare results to baseline behaviors of assumed good populations. The approach used to develop this paper is to focus on steps (1), (2) and (5). The statistics and analysis that is generated are associated with the complete set of cases that we have included in our case study analysis (Claycomb, 2012).

These incidents were queried from CERT's Non-Public Insider Incident Corpus containing nearly 1600 incidents obtained through public sources. The purpose of these cases is to give the reader an idea of the breadth of the different inside incidents in airlines and transportation sector that we have analyzed. These cases involve a variety of different organizations, technical detail, and financial impact, recovery cost, and methods used for detection. The non-aviation transportation incidents selected for this analysis reflect incidents that were the most likely to affect the aviation sector. In other words, incidents where an insider attempted to form their own business were removed from consideration given how unlikely that would be in the airline industry.

Though media reports of arrests of airline employee run the gamut from simple theft to drug trafficking to terrorist-inspired threats, they do not all meet the standard of information system involvement that warrants inclusion in the CERT Insider Threat Incident Corpus.

In the two incidents categorized as Miscellaneous, one incident involved attempted terrorism and the other involved unauthorized disclosure of personally identifiable information (PII).

4.1. Cases of Insider Threat Involving the Airline Industry

Appendix A describes the very basic summary of 10 cases associated with insiders with ties to the airline industry Internet taken from almost 1600 cases that we have obtained through public records such as

court documents and through our relationships with partner agencies and organizations. The full summary of the cases is available by contacting the authors. Interestingly, we determined there were seven additional cases in our corpus that were too recent to be included in our analysis. We hope to analyze the additional cases as follow-on work to this paper.

4.2. Insider Incident Metrics

Confidentiality was impacted in 50% of incidents. Integrity was impacted in 50% of incidents. Availability was impacted in 30% of incidents. Confidentiality and integrity were both impacted in one incident. Integrity and availability were both impacted in two incidents.

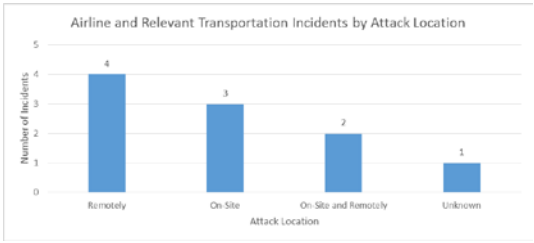

Figure 4. Attack Location

Attack location was known in 90% of incidents in the sample. Remote access was used in 60% of the incidents and on-site access was used in 50% of the incidents, with two incidents involving both remote and on-site access.

Attack Time

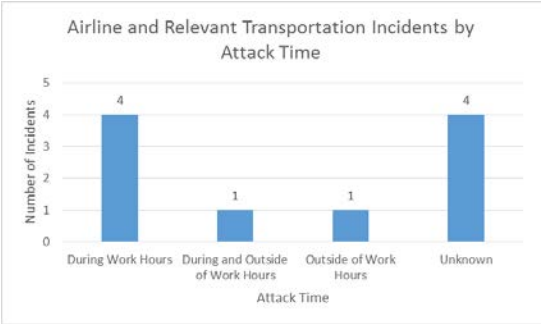

Figure 5. Attack Location

Attack time was known in 60% of the incidents in the sample. Insiders attacked during work hours in 50% of incidents and outside of work hours in 20% of incidents, with one incident where the attack took place during and outsider of work hours.

In incidents where the insider's gender was known (90%), the insider was male.

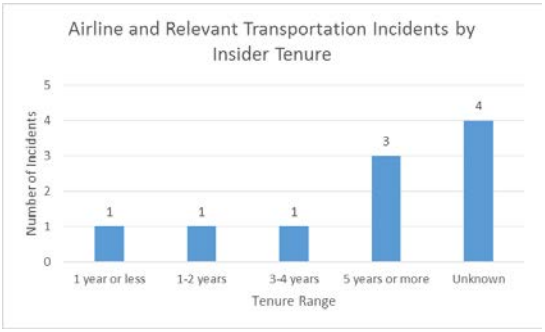

Figure 6. Insider Tenure

Although insider tenure was known in only 60% of incidents in the sample, it is interesting to note that half of those insiders had been with a victim organization for five years or more. In fact, those insiders had tenure of 6, 17, and 25 years respectively.

Figure 7. Insider Age

Given the tenure ranges of the insiders, it follows that at least half of the insiders would be at least 31 years old.

There was only one incident where an insider was associated with organized crime and no incidents where an insider was involved with the Internet underground. However, there were two instances (20%) where an insider took part in collusion with outsiders. There were no incidents that were known to involve insider accomplices.

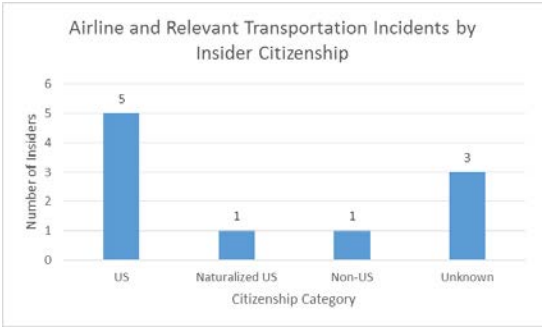

Figure 8. Insider Citizenship

Half of the insiders were US citizens, with an additional insider that was a naturalized citizen. In the three incidents where citizenship was unknown, one insider was unidentified / unnamed, another was prosecuted at the state level (so the information was unavailable), and the third was likely a US native, but this has yet to be confirmed.

The one incident where the insider was not a US citizen was the only foreign case in the sample. However, the insider was a non-citizen in the country where the incident took place.

4.3. Insider Incident Precursors

Fifty-percent of incidents in the sample were precipitated by the termination of an insider's employment. Twenty-percent of cases were precipitated by a confrontation involving the insider. (Two incidents involved both termination and confrontation.) Other precursors across the remaining 5 incidents were unique, i.e., passed over, unexplained wealth, relocation, etc.

4.4. Insiders Motive

Incidents involving the airline industry and the transportation industry (where relevant) were motivated primarily by revenge (40%), the benefit of a foreign entity (20%), and labor disputes (20%).

5. Cyber-Safety Risk Management Approaches

5.1. Promote Cyber-Safety Culture

Some of the most effective solutions to seemingly technical problems are not technical at all. They involve paradigm/mindset shifts that reveal new approaches to old challenges. One of the most powerful approaches to cyber-safety risk management would be to broaden the current safety culture paradigm beyond realm of malfunctions and mistakes, to cyber-safety. The safety culture and mindset adopted by the US aviation industry has produced a continuing downward trend in airline accidents over the past half-century, as shown in Figure 4 (McCarthy, 2018).

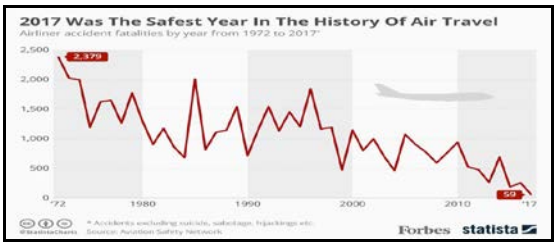

Figure 9. Airliner Accident Fatalities by year from 1972 to 2017

The Aviation Safety Network (ASN), an independent global aviation safety data resource, stated that 2017 was "the safest year ever, both by the number of fatal accidents as well as in terms of fatalities" (Shepardson, 2018). These impressive safety records can be directly attributed to the aviation safety culture cultivated over many decades (Air Transport Action Group). Updating this safety culture by adding a focus on cyber-safety will promote appropriately more skeptical, circumspect attitudes across the spectrum of operations, enabling and empowering a trust-but-verify approach to communications, navigation, weather data, and even flight-instrument displays. The key will be to think beyond troubleshooting faults and anticipating predictable failure modes & effects to incorporating a sensitivity to intentional deception, manipulation, and misdirection, as well as a realization of the connected machine-to-machine environment that modern and future aircrews will operate in. Throughout their training, pilots are imbued with the concept of attention management, i.e. knowing what to pay attention to and how much focus to apply at various times and states of flight (Stephens, et al., 2017). A new concept and practice of aviation "Trust Management" may be well worth exploring.

5.2. Creative Aviation Cyber-Safety Standards

There is a significant infrastructure, vibrant community, and comprehensive body of aviation safety standards. The International Civil Aviation Organization began developing, updating, and publishing extensive Standards and Recommended Practices (SARP) on Safety Management in 2001, and considers safety "at the core of ICAO's fundamental objectives" (International Civil Aeronautical Organization, n.d., p. 1). The FAA Office of Safety Standards establishes safety standards across the spectrum of ground and flight

operations, technology, and safety promotion (US Federal Aviation Administration, 2017). These national and international safety governance bodies are supported by various industry groups, such as the International Air Transport Association (IATA) and the US-based RTCA (formerly, Radio Technical Commission on Aeronautics) (RTCA, 2018). Fortunately, these organizations have recently begun to address cyber-safety challenges. The ICAO issued a *Declaration on Cybersecurity in Civil Aviation*, at its first Cyber Summit, in 2017, with a specific call for "increasing the resilience of the global aviation system against cyber-threats that may jeopardize the safety…of civil aviation" (International Civil Aviation Organization, 2017, p. 1). The FAA, launching a multi-year effort to manage cyber-safety risks, assembled an Advisory Committee in 2015 to "develop standards and safeguards designed to detect, track and isolate data intrusions and other cyber-attacks against aviation" (Edwards, 2016, p. 1). The RTCA Special Committee 216: Aeronautical Systems Security, is now addressing cyber safety as well, with the expressed intent to "help ensure safe, secure and efficient operations amid the growing use of highly integrated electronic systems and network technologies used on-board aircraft" (RTCA, 2018).

5.3. Adopt, Adapt, and Extend Terrestrial Cyber Risk Mitigation Technologies

There are many well-developed and emerging technical approaches to mitigating terrestrial cyber risks. These technologies are aimed at mitigating risks to information confidentiality, integrity, and availability. Though confidentiality compromise is not necessarily a cyber-safety risk, integrity and availability of data and communication channels can be vital to safe flight. The US Industrial Control System Computer Emergency Response Team (ICS-CERT) has suggested some of these technical approaches. They include network segmentation, firewalls, encrypted remote access, role-based access controls, system logging, continuous patching and updating, and compromise detection & alerting (US Computer Emergency Response Team, 2015).

Technical approaches to IoT cybersecurity are highly applicable to aviation cyber-safety due to the tremendous growth in aircraft-embedded IoT devices. In their new book, *Solutions for Cyber-Physical Systems Ubiquity*, Austrian researcher Druml Norbert and his colleagues suggest a new technical approach, employing "self-adaptive software systems" may significantly increase IoT security via capabilities to "detect security attacks and isolate the infected devices or block the attackers" (Druml, Genser, Krieg, Menghin, & Hoeller, 2018, p. 312).

These three technical approaches to cyber risk mitigation are a small sampling of the many opportunities to for the aviation community to adopt, adapt, and extend terrestrial approaches to aviation cyber-safety. They point to a rich and vital area for further investment, research, and development.

6. Summary

This report attempted to narrow the knowledge gap of the cyber-physical safety (cyber-safety) risks attending The Connected Aircraft. It has shown that Connected Aircraft are, indeed, cyber-physical systems and has summarized three examples of airborne systems with significant cyber-safety risks: Integrated Modular Avionics Systems, Full Authority Digital Engine Controls, and next-generation aviation Health Management Systems. Next, it discussed the concept of the threat from within and how the interconnected aircraft can be especially vulnerable to insider attacks. Further, three approaches to cyber-safety risk management: building a cyber-safety culture, creating and promoting aviation cyber-safety standards, and adopting, adapting, and extending terrestrial cyber risk mitigation technologies to airborne cyber-physical systems, were also presented. Proactive work is underway and a great deal of vital investment, research, and experimentation lies ahead to protect Connected Aircraft and the traveling public from exposure to unacceptable cyber-safety risk.

7. References

Don't forget to cite the figures and any new insider threat cases. The below references are in order of when they appear but are not complete. Be sure to add brackets before and after the number when you are completely done.

[1] Griffor, Edward, ed. *Handbook of system safety and security: cyber risk and risk management, cyber security, threat analysis, functional safety, software systems, and cyber physical systems*. Syngress, 2016.

[2] Sampigethaya, Krishna, and Radha Poovendran. "Aviation cyber–physical systems: Foundations for future aircraft and air transport." *Proceedings of the IEEE* 101.8 (2013): 1834-1855.

[3] Ramsey, James W. "Integrated Modular Avionics: Less is more-Fresh approaches to integrated modular avionic architectures will save weight, improve reliability of A380 and B787 systems." *Avionics Magazine* 31.2 (2007): 24.

[4] Cyber Security Intelligence Ltd. (2015, June 1). *Hacker's Into Commercial Airline Systems*. Retrieved from CybersecurityIntelligence.com: https://www.cybersecurityintelligence.com/blog/hackers-into-commercial-airline-systems-327.html

[5] Slavov, K., Migault, D., & Pourzandi, M. (2015, August 31). *Identifying and addressing the vulnerabilities and security issues of SDN*. Retrieved from Ericsson.com: https://www.ericsson.com/en/publications/ericsson-technology-review/archive/2015/identifying-and-addressing-the-vulnerabilities-and-security-issues-of-sdn

[6] McAfee, J. (2016, January 17). *JOHN MCAFEE: We aren't talking enough about cybersecurity*. Retrieved from BusinessInsider.com: http://www.businessinsider.com/john-mcafee-we-arent-talking-enough-about-cybersecurity-2016-1?IR=T&r=US&IR=T

[7] GAO. (2015, April). *FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*. Retrieved from GAO.gov: https://www.gao.gov/assets/670/669627.pdf

[8] Zetter, K. (2015, May 15). *Feds Say That Banned Researcher Commandeered a Plane*. Retrieved from Wired.com: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

[9] Biesecker, C. (2017, November 8). *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*. Retrieved from Aviationtoday.com: http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/

[10] Paganini, P. (2017, November 13). *DHS – Tests demonstrate Boeing 757 airplanes vulnerable to hacking.* Retrieved from SecurityAffairs.co: http://securityaffairs.co/wordpress/65463/hacking/dhs-boeing-757-hacking.html

[11] SCRIBD. (2018, February 10). FADEC_Full-Authority Digital Engine Control. Retrieved from Scribd.com: https://www.scribd.com/doc/47618375/FADEC-Full-Authority-Digital-Engine-Control

[12] Sizemore, A. (2017, December 28). *ADS-B and Aviation Cybersecurity: Should Passengers Be Concerned?* Retrieved from SecurityIntelligence.com: https://securityintelligence.com/ads-b-and-aviation-cybersecurity-should-passengers-be-concerned/

[13] Storm, D. (2012, August 1). *Curious Hackers Inject Ghost Airplanes into Radar, Trak Celebrities' Flights.* Retrieved from Computerworld.com: https://www.computerworld.com/article/2472455/cybercrime-hacking/curious-hackers-inject-ghost-airplanes-into-radar--track-celebrities--flights.html

[14] Zimmerman, J. (2013, January 17). *ADS-B 101: what it is and why you should care.* Retrieved from AirFactsJournal.com: https://airfactsjournal.com/2013/01/ads-b-101-what-it-is-and-why-you-should-care/

[15] Costin, A., & Francillon, A. (2012). *Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on.* Retrieved from Blackhat.com: https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf

[16] Boeing Corp. (2013). *Connected Flight.* Retrieved from 787updates.newairplane.com: http://787updates.newairplane.com/24-7-Customer-Support/Connected-Flight

[17] Bellamy, III, W. (2017, February 15). *OEMs Embrace New Aircraft Engine Health Monitoring Tech.* Retrieved from aviationtoday.com: http://www.aviationtoday.com/2017/02/15/oems-embrace-new-aircraft-engine-health-monitoring-tech/

[18] Shepardson, D. (2018, January 1). *2017 safest year on record for commercial passenger air travel: groups.* Retrieved from Forbes.com: https://www.reuters.com/article/us-aviation-safety/2017-safest-year-on-record-for-commercial-passenger-air-travel-groups-idUSKBN1EQ17L

[19] Air Transport Action Group. (n.d.). *Aviation Benefits Beyond Boarders: Safety Culture.* Retrieved March 2, 2018, from aviationbenefits.org: https://aviationbenefits.org/social-development/safety-culture/

[20] Stephens, C., Harrivel, A., Prinzel, L., Comstock, R., Abraham, N., & Pope, A. (2017). *CREW STATE MONITORING AND LINE-ORIENTED FLIGHT TRAINING FOR ATTENTION MANAGEMENT.* Retrieved from NTRS.NASA.gov: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170005473.pdf

[21] McCarthy, N. (2018, January 2). *2017 Was The Safest Year In The History Of Commercial Air Travel*

[Infographic]. Retrieved from Travelwirenews.com: http://travelwirenews.com/2017-was-the-safest-year-in-the-history-of-commercial-air-travel-infographic-609863/

[22] International Civil Aviation Organization. (2017). *DECLARATION ON CYBERSECURITY IN CIVIL AVIATION DUBAI, UNITED ARAB EMIRATES 4 TO 6 APRIL 2017 (DRAFT).* Retrieved from ICAO.int: https://www.icao.int/Meetings/CYBER2017/Documents/Final%20text%20Declaration%20(2).pdf

[23] US Federal Aviation Administration. (2017, August 18). *Office of Safety Standards*. Retrieved from Faa.gov: https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/

[24] RTCA. (2018). *SC-216, Aeronautical Systems Security.* Retrieved from RTCA.org: https://www.rtca.org/content/sc-216

[25] International Civil Aviation Organization. (2017). *DECLARATION ON CYBERSECURITY IN CIVIL AVIATION DUBAI, UNITED ARAB EMIRATES 4 TO 6 APRIL 2017 (DRAFT).* Retrieved from ICAO.int: https://www.icao.int/Meetings/CYBER2017/Documents/Final%20text%20Declaration%20(2).pdf

[26] Edwards, J. (2016, June 20). *FAA Panel Drafts Cybersecurity Standards for Commercial Aircraft Operators.* Retrieved from executive.gov: http://www.executivegov.com/2016/06/faa-panel-drafts-cybersecurity-standards-for-commercial-aircraft-operators/

[27] US Computer Emergency Response Team. (2015, June). *10 Basis Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks.* Retrieved from ICS.CERT.US-CERT.gov: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

[28] Druml, N., Genser, A., Krieg, A., Menghin, M., & Hoeller, A. (2018). *Solutions for Cyber-Physical Systems Ubiquity.* Hershey PA, USA: IGI Global.

[29] Claycomb, William R., et al. "Chronological examination of insider threat sabotage: preliminary observations." Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 3.4 (2012): 4-20.