Cyber Security in Civilian Aviation: Insights for Advanced Nuclear Technologies

Charalampos Andreades
James Kendrick
Chris Poresky
Per Peterson

UCBTH-17-001

April 2017
Department of Nuclear Engineering
University of California, Berkeley

This research is being performed using funding received from the Center for Long-Term Cybersecurity of the University of California, Berkeley.

Abstract

This report provides a brief overview of legacy avionics and the air traffic control system (ATS), describes the current Next Generation (NextGEN) ATS, the integrated modular avionics (IMA) of modern aircraft, and provide a list of potential cyber security (CS) issues and associated CS anectodotes/incidents. An overview of the civilian/commercial aviation industry regulatory framework and introduced CS measures and solutions are summarized. Finally, some short concluding remarks and discuss the relevance of aviation CS to nuclear CS are provided.

1 Introduction

In pursuit to better understand cybersecurity for digital instrumentation and control (I&C) for advanced nuclear reactors, we decided to first explore and review the approaches and strategies taken in other critical infrastructures sectors (as defined in Presidential Policy Directive 21 [1]) that face similar challenges and large consequence spaces, as does nuclear power. The aviation industry, with its heavy reliance on digitization of controls and its connection to the internet instantly sprung to mind; – another closely related example is the autonomous vehicle and its associated infrastructure and integrated transportation network. When one walks onto a modern aircraft such as the Boeing 737MAX, it is instantly noticeable to the keen observer that there are digital screens, file servers, an aircraft operating system, multiple networks and equipment, large storage drives (media, music, movies, etc.). Surprisingly, this internet protocol (IP) connected network is not always air gapped. It is important to note at the outset, that the civilian and commercial aviation industry has taken a path to full digitization, with minimal or no analog control of avionics[1] and the air traffic control services (ATS), and their grappling with the CS issue is still in its early stages and evolving, not much further along than the commercial nuclear sector. In the following sections we will give a brief summary of legacy avionics and ATS, describe the current Next Generation (NextGEN) ATS, the integrated modular avionics (IMA) of modern aircraft, and provide a list of potential CS issues and associated CS anectodotes/incidents. We conclude with an overview of the civilian/commercial aviation industry regulatory framework and introduced CS measures and solutions. Finally, we will provide some short concluding remarks and discuss the relevance of aviation CS to nuclear CS.

2 History and Summary of Legacy ATC and Avionics

Traditionally, the United States National Air Space (NAS), ATC and the associated avionics were based on federated technologies such as Satellite Based Augmentation Systems (SBAS), Global Positioning Augmentation Systems (GBAS), Air Traffic Control (ATC) data communications, Automatic Dependent Surveillance – Broadcast (ADS-B), and Controller Pilot Data Link Communications (CPDLC), that were difficult or impossible to intercept externally and were isolated and air gapped.[2] Therefore little emphasis was given to digital security other than physical access control [2]. The system and legacy devices were regulated by deferral agencies with uniform security standards. However, with the progress in digital technology, non-ATS, non-Federal Aviation Administration (FAA) regulated systems with variable security standards (Wi-

[1] Avionics is a combination of the terms aviation and electronics. They are the electronic systems used on aircraft, which include communications, navigation, the display and management of multiple systems, and the hundreds of systems that are fitted to aircraft to perform individual functions.

[2] Internationally, the International Civil Aviation Organization (ICAO), is a specialized agency of the United Nations, which codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth. The ICAO Council adopts standards and recommended practices concerning air navigation, its infrastructure, flight inspection, prevention of unlawful interference, and facilitation of border-crossing procedures for international civil aviation.

Fi, WiMAX, Ethernet, gate linked networks, portable electronic devices, USB, maintenance laptops, etc.) have been introduced into aviation.

3 Path to NextGEN ATS

In the past twenty years or so, the introduction of more powerful and compact processing systems, following Moore's law, have led the aviation industry to advocate for the modernization of the NAS and the formation of the NextGEN ATS, a move from radar based ATC to one based on satellite navigation (GPS) and automation. This has been an incremental adoption of enterprise information technology (IT), mixed in with legacy federated systems. What is envisioned through NextGEN is an e-enabled aircraft in a self-aware airborne mode in a global information network, sourcing and consuming the right information at the right place and time [3]. Internet signals are routed through existing communications architecture while aircraft controls move from federated separate control units per function to an integrated modular avionics (IMA) platform. The concept of modern digital avionics originated in the late 1980s in the McDonnell Douglas F-15E program and later adopted in civilian and commercial aviation during the 1990s in the Boeing 777.

The move to fly-by-wire was initially introduced as a back-p to mechanical control until all kinks were ironed out. The substitution of fly-by-wire for mechanical controls allowed for a reduction in cost and weight for aircrafts. The further digitization of avionics has led to a transition from fly-by-wire, described earlier, to a fly-by-wireless system, a digital circuit activated control by network called IMA.

4 Integrated Modular Avionics

As described in the previous section, aircraft systems and avionics have moved from a federated and distributed architecture to an IMA based architecture. IMA replaces numerous separate processing units and line replaceable units with fewer more centralized units by employing higher throughput multicore, multi-processor computers, with commercial off-the-shelf components [3, 4]. This centralization of processing power means that multiple unrelated applications with different criticalities share the same computational platform (hopefully without interference). Think of all the functions on modern airplanes: Wi-Fi, electronic flight bags[3], field loadable devices and software, avionics, passenger information and entertainment management system, and the list goes on. To accommodate this sharing of information across bidirectional high speed data buses with connectivity to many aircraft systems, modern aircraft are segregated into three logical domains based on function and criticality to flight [2, 3, 5]. These are the following:

1) Closed domain for aircraft control, communicating externally through data links and SATCOM.
2) Private domain responsible for the aircraft system information, communicating externally with flight operations and maintenance.

[3] An electronic flight bag is an electronic information management system on a portable electronic device used by pilots to replace traditional flight bags which weighed up to 40 pounds. Flight bags include safety guidelines, startup procedures, checklists, navigation charts, flight and aircraft calculations, etc. for pilots to go through and reference.

3) Public domain for passenger in-flight entertainment (IFE) and information services, connecting externally with content providers and the passengers.

What is concerning in this architecture of modern avionics is that the aircraft, the cockpit and cabin crew and passengers use many of the same communications components. An easy visualization of this is communication of aircraft flight information from the private domain to passengers' screen on the public domain (speed, altitude, ambient conditions, flight trajectory, etc.). This leads us into our next section of potential CS vulnerabilities of IMA and cases or anecdotes of CS breaches on-board.

5 Aviation Cyber security Vulnerabilities and Anecdotes

A key issue for CS of IMA is the potential that the processing of mixed criticality information by shared network components may make it possible hack from one network segment to another domain by circumventing security measures. There are several levels of attacks and various entry points one could envision. In one potential attack, one might try to misinform pilots or air traffic controllers via spoofing or jamming attacks (delete/insert ghost airplanes from/into screens, compromise information accuracy, deletion of messages/information, fake alarms, etc.). This is a particular vulnerability since place positioning date (NextGEN) is unencrypted and without mutual authentication [6]. An attacker with deep knowledge of systems and premeditation can gain fly-by-wire control and disable all communications and control systems. This is particularly so in the Boeing 777 where controls could be obtained with a radio signal from a small device. This is a speculated cause of the Malaysia Airlines flight MH370 disappearance. This scenario was demonstrated as a credible one by CS researcher Hugo Teso, who created an Android phone application, SIMON, to gain remote control access to flight controls [6]. He developed the application using a commercially available flight simulator, pointing to another vulnerability, that of monoculture. Monoculture is the use of either widely available software or wide use of software across networks, resulting in wide knowledge of system architecture or operation, unchanged default logons and passwords, etc. [7].

Another attack vector is the possibility of the IFE connection to the private domain to be externally exploited via USB ports and Ethernet. The Boeing 787's passenger compartment was connected to the aircraft's control domain, navigation, and communications system directly. Security researcher Chris Roberts exploited this vulnerability by plugging his laptop into the under-seat IFE box and managing to yaw the airplane, all the while tweeting about it [8, 9].

System integration might also enable a rogue or coerced employee to circumvent physical access control and inject malware aboard the IMA network. Spainair flight 5022 on August 20, 2008 crashed due to computer system monitoring technical problems caused by malware infections, resulting in 154 deaths [10].

All these theorized, potential, realized CS vulnerabilities and anecdotes demonstrate that CS is indeed a matter to be addressed seriously in the aviation industry, leading us into our next section on aviation CS measures, defense, and regulatory framework.

6 Aircraft CS Regulatory Framework and Solutions

The move to NextGEN and IMA has meant that new CS features need to be adopted to prevent attack and mitigate consequences in case of a breach, and that a new regulatory framework be put in place to provide guidance for CS to aviation industry stakeholders. Currently, the industry in the U.S. operates under a patchwork of CS regulations with no overarching set of rules from a defined body, e.g. the FAA. In April 2016, the United States Congress passed the Cyber Air Act, with the precise intention of the FAA to develop these CS guidelines [8]. Under the broadest layer of safety and regulations, aircraft need to comply with 14CFR 129.25, 129.28, 25.795 and CS control conform to 14CFR xx.1301 and xx.1309 [2]. NIST SP800-30 (risk management for IT systems), RTCA SC216, DO326, DO178C (for software), DO254 (for hardware), and DO297 (for IMA) provide both software and hardware security and SC guidance and requirements [2]. IMA logical domain separation security is guided by ARINC 653, an industrial standard for integrity of safety-critical IMA application cohosted with less critical applications by partitioning the operating system [3]. Partitioning is provided through a time-triggered Ethernet protocol separating critical and non-critical communications through predefined time slots on the network, allowing multiple traffic classes to coexist [4]. Additionally, ARINC 811 provides mechanisms to protect flight critical systems. However, all these standards are not under FAA control and aircraft worthiness certification, performed by the Office of Safety, (similar to U.S. Nuclear Regulatory Commission reactor design certification) does not include an explicit CS assessment component. CS issues, if discovered or if they arise, as they did with the Airbus A350 and Boeing 787, are addressed by rulings called Special Conditions, that apply to each particular case rather than across the board [11]. This implies that commercial grade SW and HW cannot be assured under current aviation safety regulations (valid as of 2017 – rulemaking procedure underway) [3, 11].

Looking into these standard and regulation once can distill some basic concepts, recommendations, and mandates as to how to address CS in modern avionics. First and foremost, aircraft security relies on redundancy and determinism with human element involvement. The concept of defense-in-depth is applied on aircraft systems, with redundancy, back-ups, and fail-safe modes, in which the system reverts to manual control or a known safe configuration in the event of an anomaly. On the SW and HW side, firewalls serve as a first line of electronic defense to protect flight controls from other domains. This approach is vulnerable to circumvention however, since the domains are connected with the same IP communication and routers. The use of different communications standards could make control and monitoring incompatible, however this is not implements in practice yet. To further fortify IMA, cross-domain communications are secured at multiple layers using sufficient physical, logical, and organizational inhibitors (routers, switches, monitors, usage policies for wireless devices, etc.) Other host-based mechanisms (filtering, redundant storage, tamper proof logging of security-relevant actions) ensure that the flight control domain is operational and close to the passenger domain [12]. The Boeing 787 and Airbus A380 us an open redundant network topology for their avionics [4]. This certified control information flow between domains, maintained by network extension devices, ensures that an attacker would have to affect multiple systems to reduce safety margins. This implies that an attacker might prefer to misguide information rather than cause a loss of function. This attack vector is dealt with in a two-fold manner – with some legacy capability and human factor security.

The use of back-up hardwired or legacy connections for safety critical information can enable cross checks for verifying wireless readings and mitigating attack consequences. The Traffic Collision Avoidance System (TCAS – radar based) can back up the Automatic Dependent Surveillance – Broadcast (ADS-B – GPS based), so that a degraded GPS signal can be augmented by a secondary legacy radar based, albeit less accurate, system [3, 12].

On the human factor of CS, pilots are trained time and again on handling system problems (similar to nuclear reactor operators). They can disengage, disconnect, and ignore a malfunctioning system. Additionally, there is redundancy for human control in which pilots and co-captains can recognize a bogus message, by requiring pilot review and approval for major changes (similar to three way communication for nuclear reactor operators) [10]. There is furthermore role based access to avionics systems, with security permissions based on the user's position or function (insider vs. outsider) [11].

This entire CS architecture needs to be tested against threats and verified using rigorous mathematical reasoning and advanced analysis tools to reduce or eliminate vulnerabilities [5]. Built-in test software, real-time monitors, and triplicate voting mechanisms that could detect and isolate most IC malfunctions/failures from inadvertent or intentional degradation are either implemented or proposed [2]. It is also important not to neglect the other components outside the aircraft and take a system-wide approach to CS. For example, counterfeit parts need to be detected and eliminated during the procurement and tracking process prior to going on-board aircraft. This system-wide approach can be considered as a combination of defense-in-depth and security by design (proactive rather than reactive).

7 Relevance to Advanced Nuclear and Conclusions

In reviewing aircraft avionics and the migration to a fully networked fly-by-wireless architecture, several implications for CS can be identified. There is a very little to no analog control envisioned in future aircraft other than for redundancy purposes. Civilian aviation regulations are starting to catch up with the CS issues, but threats remain a constantly evolving issue requiring constant vigilance and updating. In aviation, as in nuclear power, CS, physical security, and safety need to be coordinated in a risk informed approach. The aviation sector has implemented security controls such as access control, contingency planning (including a human element), and physical security measures to buttress against potential cyber-attacks. Retention of back-ups, mitigations against spoofing, built-in cross-checks of surveillance data and encryption provide assurance that the move to IMA will maintain a similar level of CS as for previous generation of digital avionics, while conferring added functionality and benefits. These approaches, if not already applied in nuclear I&C, can be adopted when and where applicable.

More specific to advanced nuclear controls research at Berkeley using the CIET facility, we plan to study how the Airborne Network Security Simulator (ANSS) at Witchita State can provide guidance, lessons, and applicable examples to CS experiments for CIET. "ANSS integrates industry and government aeronautical simulator to assess and identify network security threats in airborne network environments and provides a security test-bed used to test, calibrate, exercise procedures, and assess potential weaknesses and vulnerabilities, without endangering people or resources." [13]

Acronyms and Abbreviations

ADS-B – Automatic Dependent Surveillance – Broadcast

ANSS – Airborne Network Security Simulator

ATC – Air Traffic Control

ATS – Air traffic control services

CPDLC – Controller Pilot Data Link Communications

CS – Cyber security

FAA – Federal Aviation Administration

GBAS – Global Positioning Augmentation Systems

HW – Hardware

ICAO – International Civil Aviation Organization

IFE – In-flight entertainment

IMA – Integrated modular avionics

IP – Internet protocol

IT – Information technology

I&C – Instrumentation and control

SBAS – Satellite Based Augmentation Systems

SW – Software

TCAS – Traffic Collision Avoidance System

8 References

[1] Office of the Press Secretary, "Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience," The White House, Washington, DC, February 12, 2013.

[2] P. Skaves, "Information for Cyber Security Issues Related to Aircraft Systems," in *30th Digital Avionics Systems Conference, IEEE*, Washington, DC, October 16-20, 2011.

[3] K. Sampigethaya and R. Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE,* vol. 101, no. 8, pp. 1834-1855, August 2013.

[4] T. Gaska, C. Watkin and Y. Chen, "Integrated Modular Avionics-Past, present, and future," *IEEE Aerospace and Electronic Systems Magazine ,* vol. 30, no. 9, pp. 12-23, 2015.

[5] K. L. Statler, "Cybersecurity And The Commercial Aircraft — Delivering Leading-Edge Technology To Meet A Growing Threat," AviationWeek.com, 30 June 2016. [Online]. Available: http://aviationweek.com/information-management-solutions/cybersecurity-and-commercial-aircraft-delivering-leading-edge-techn. [Accessed 15 February 2017].

[6] P. Paganini, "Cyber Threats against the Aviation Industry," Infosec Institute, 8 April 2014. [Online]. Available: http://resources.infosecinstitute.com/cyber-threats-aviation-industry/#gref. [Accessed 15 February 2017].

[7] R. A. Grimes, "Can you hack an airplane? Brace yourself," InfoWorld, 21 April 2015. [Online]. Available: http://www.infoworld.com/article/2912372/security/can-you-hack-an-airplane.html. [Accessed 15 February 2017].

[8] J. Wolff, "Hacking Airplanes," Slate, 3 May 2016. [Online]. Available: http://www.slate.com/articles/technology/future_tense/2016/05/the_aviation_industry_is_starting_to_grapple_with_cybersecurity.html. [Accessed 15 February 2017].

[9] Phys.org, "Is cyberjacking a new threat to air travel?," Phys.org, 13 July 2015. [Online]. Available: https://phys.org/news/2015-07-cyberjacking-threat-air.html. [Accessed 15 February 2017].

[10] R. Abeyratne, "Aviation Cyber Security: A Constructive Look at the Work of ICAO," *Air and Space Law,* vol. 41, no. 1, pp. 25-39, 2016.

[11] U.S. Government Accountability Office, "AIR TRAFFIC CONTROL: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen," GAO-15-370, Washington, DC, April 14, 2015.

[12] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proceedings of the IEEE,* vol. 99, no. 11, pp. 2040-2055, 2011.

[13] R. De Cerchio and C. Riley, "Aircraft systems cyber security," in *30th Digital Avionics Systems Conference, IEEE*, Washington, DC, October 16-20, 2011.

9 Other Bibliography

[14] Gulliver, "Hacking aircraft: Remote control," *The Economist,* 4 11 2014.

[15] T. Fox-Brewster, "Hacking planes - UK researchers developing plans to stop 'flight cyberjacking'," *The Guardian,* 4 11 2014.

[16] M. Pierides, B. E. Finch, R. Azim-Khan and S. P. Farmer, "Cybersecurity and the Aviation Sector: Recent Incidents Highlight Unique Risks," Pillsbury Law, 24 August 2015. [Online]. Available: https://www.pillsburylaw.com/en/news-and-insights/cybersecurity-and-the-aviation-sector-recent-incidents-highlight.html. [Accessed 15 February 2017].

[17] R. Santamarta, "Here be backdoors: A journey into the secrets of industrial firmware," in *Black Hat USA*, Las Vegas, NV, 2012.