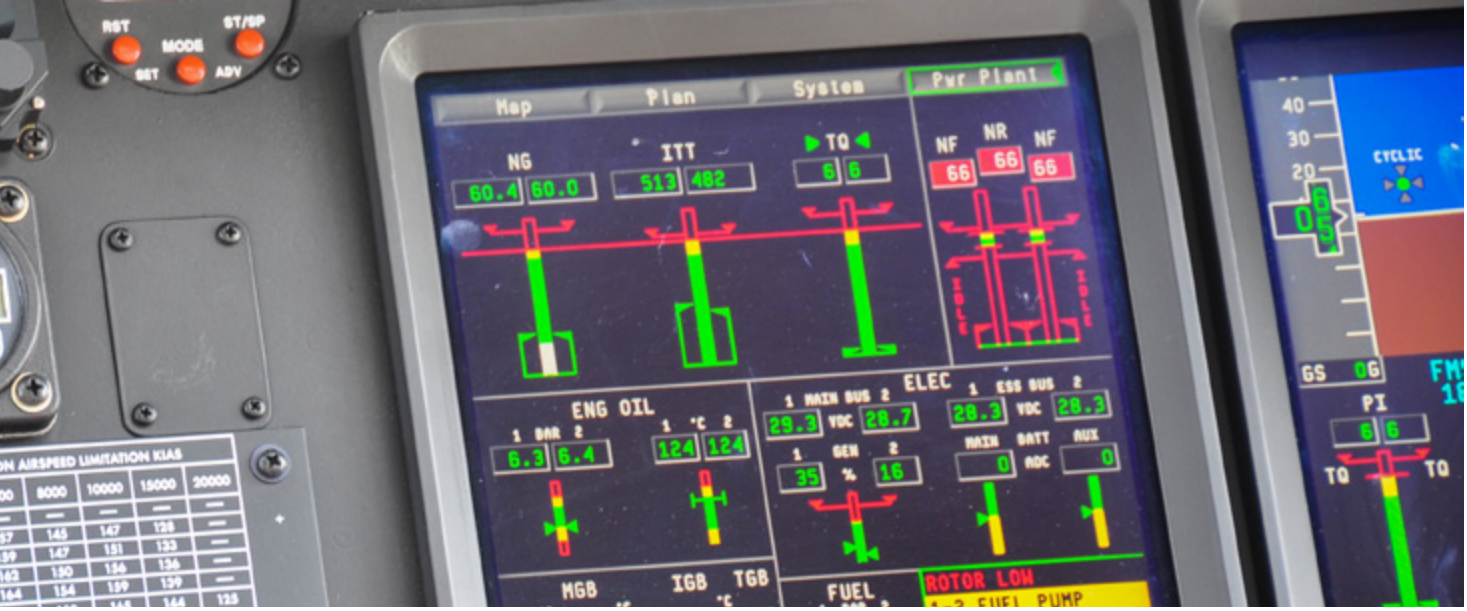
ALPA WHITE PAPER

Air Line Pilots Association, Int'l
1625 Massachusetts Ave., NW
Washington, DC 20036
703-481-4440
Media@alpa.org • www.alpa.org

JUNE 2017

AIRCRAFT CYBERSECURITY: THE PILOT'S PERSPECTIVE



Introduction

The risks encountered in flying are frequently mitigated by the knowledge, training, and experience of the professional pilot. As new safety risks are discovered, the aviation community resolves to overcome these safety deficiencies through improvements to our aviation system, whether it be related to air traffic services, airport and ground operations, aircraft design, or advances in aeronautical knowledge and training of the flight and cabin crew. The results of the government and industry's joint efforts speak for themselves as evidenced by the fact that airline travel is currently the safest mode of transportation.

A key component to the increased safety of aviation, namely highly advanced onboard information technology (IT) systems, is also ironically a cause for concern as the systems pose the potential for creating a cybersecurity threat which could impair safety of flight. Historically, aircraft data used for operational purposes came from reliable, known sources, such as issued flight plans, Air Traffic Control (ATC) radio transmissions, company messages via Aircraft Communications Addressing and Reporting System (ACARS), and navigation and software updates performed by maintenance technicians.

For the last two decades, however, aircraft systems design has advanced to meet the airlines' increasing needs for performance and capability, which includes data from numerous external sources such as satellites, cell service, Wi-Fi, portable electronic devices, and others. The integration of onboard information and communications technology increasingly requires careful design and procedures to ensure the safe and secure operation of the aircraft.

The current generation of commercial aircraft—commonly referred to as "E-enabled" aircraft—have integrated IT network technologies that are replete with convenience and efficiency. Advanced IT systems located within E-enabled aircraft comprise sophisticated onboard networks that rival the capability and performance of ground-based networks.

E-enabled aircraft systems increasingly rely on multiple paths of connectivity with external networks to routinely communicate, exchanging data during flight or while on the ground, from any geographic location. Examples of such data communications include:

- Uploading and downloading large amounts of flight and system data, to include in-flight entertainment using wireless technology.
- Performing maintenance testing and diagnostic functions remotely.
- Equipping engines with "call home" functions for trend and operational information.
- Implementing wireless communications (e.g., SATCOM, HF, VHF, IFE, Wi-Fi, and cellular, etc.) which include software updates for any onboard communications avionics.

The Cybersecurity Threat to Airline Aircraft

Aircraft interact with countless different networks around the globe, all with varying degrees of security, so cyber attacks pose an ongoing threat to aircraft. However, experts within the government and industry have expressed somewhat divergent views about the potential for such threats to be realized. Some believe that the risk posed by this threat is minimal and is addressed during the manufacturing process and by operational safeguards, while others see the potential for hackers to circumvent security measures and create unsafe flight conditions.

Possible threats to aircraft operations via electronic means may come in a variety of ways. Honeywell Aerospace has identified basic forms of cybersecurity threats[1] which include the following:

Spoofing

- Modifying data that otherwise appears to be from a legitimate source
- Using protocol weaknesses, compromised security data, or compromised ground systems

Exploiting

- Using a digital connection to execute malicious instructions on installed equipment
- Using software vulnerabilities

Denial of Service

- Using a digital connection to disrupt service

Counterfeiting

- Inserting malicious content into a legitimate part, software component, or database

[1] "Civil Aviation and CyberSecurity," Dr. Daniel P. Johnson, Honeywell Aerospace Advanced Technology, 2013

The U.S. Air Force[2] has identified potential cybersecurity attack modes and outcomes in numerous systems, including the following:

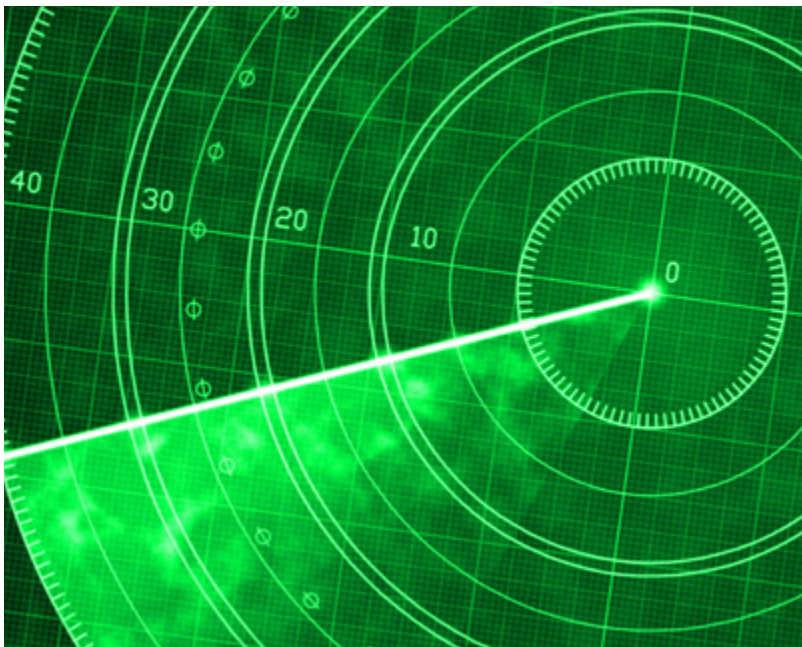
Communications Systems

- Connections with "rogue" frequency/channel/link without user knowledge
- Broadcasting voice/data over nonsecure or secure frequency/channel/link without user knowledge
- Forcing a microphone into a "hot mic" situation
- Injecting false messages into systems or data link communications
- Injecting a cyber payload via datalink that targets an onboard system

Navigation and Flight Instrument Systems

- Disabling, spoofing, or degrading GPS accuracy/reading
- Corrupting aircraft orientation indicators to mislead flight crew

[2] "Managing Cybersecurity Risk in Weapon Systems" Dr. Raju Patel, Aircraft Systems Authorizing Official, US AIR FORCE, LCMC, March 21, 2017



Flight Control Systems

- Injecting flight control inputs to roll/pitch/yaw
- Denying or limit responsiveness to user flight control inputs to roll/pitch/yaw

Traffic and Terrain Safety Warning Systems

- Add/remove/change location of aircraft
- Add/remove/change location of terrain or ground obstacles
- Overload with "noise" data to make unusable
- Corrupt system indicators to mislead flight crew about system status

Aircraft Health and Usage Monitoring Systems

- Indicate repairs required when none are necessary
- Indicate lower/fewer, higher/more, or different repairs are required than necessary
- Indicate aircraft OK when repairs are necessary

Air Traffic Networks

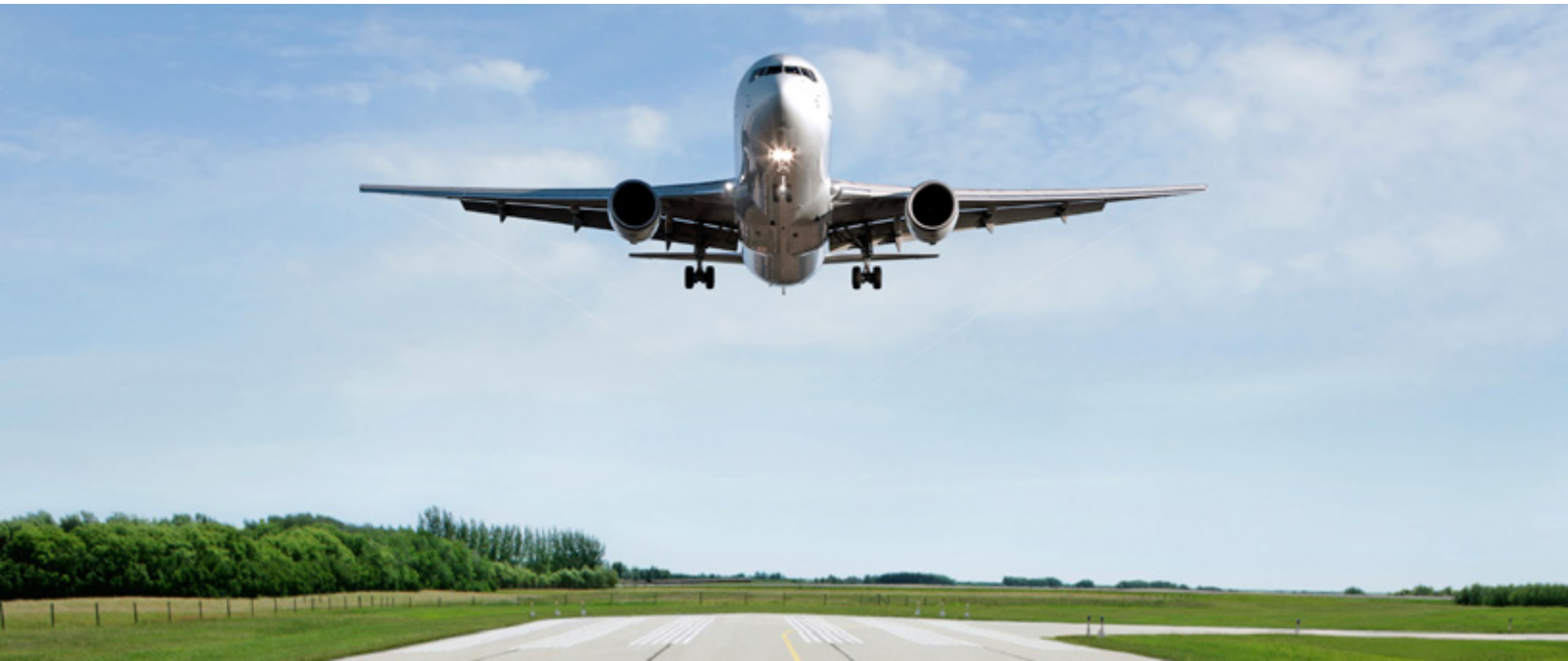
- Air Traffic Control systems compromised, passwords stolen, malware installed, false messages to pilots, fake distress calls, etc.

Automatic Dependent Surveillance-Broadcast

- Create phantom aircraft
- Limited security in the system protocol
- Create fake weather reports
- Jamming
- Transmit wrong/misleading information to pilots and air traffic controllers

ACARS

- Bogus flight plan update
- False weather information
- Fake messages between aircraft and ground



Aircraft Cybersecurity Requirements

In December 2014, the U.S. Aviation Rulemaking Advisory Committee (ARAC) accepted a proposed tasking from the FAA to "provide recommendations regarding Aircraft Systems Information Security/Protection [ASISP] rulemaking, policy, and guidance on best practices for airplanes and rotorcraft, including both certification and continued airworthiness" to address vulnerabilities and identify mitigations. ARAC completed its report to the FAA in August 2016 containing the result of its deliberations which stated, in part, that the current federal aviation regulations do not define how to address electronic cybersecurity vulnerabilities.

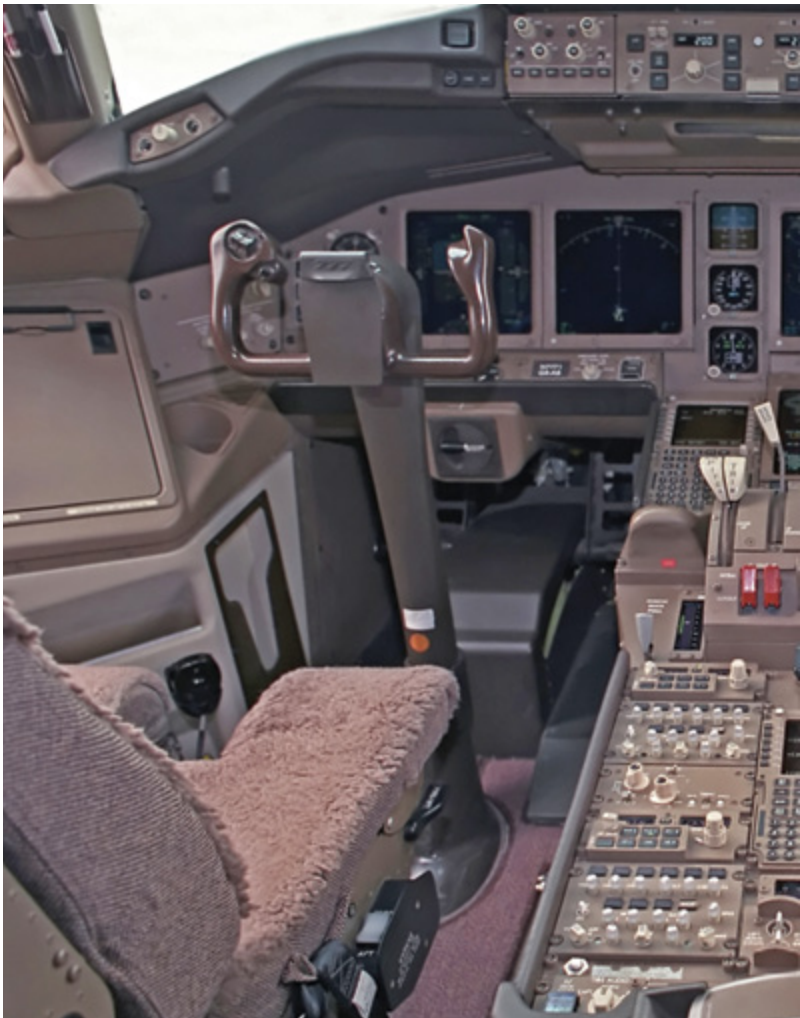
Recommendations included in the report call for, among other things, a new provision in 14 CFR Part 25, Airworthiness Standards for Transport Category Aircraft, which would require manufacturers to protect airplane equipment, systems, and networks from intentional unauthorized electronic interactions. Presently, FAA addresses aircraft cybersecurity needs with published "special conditions" for specific make and model aircraft designs to protect aircraft when connected to external services or networks under specific conditions.

A cyber attack could take place through several vectors to exploit onboard IT networks and aircraft systems used to manage all flight-operation activities, including flight control and navigation systems, not just communications.[3] Developing technologies that protect the entire flight operation is a tremendous challenge, especially with an aircraft that transmits and receives through multiple communications, surveillance, and navigation technologies that cross-tie into other systems.

There is broad agreement within the government and industry that mitigations are required to protect against cybersecurity attacks onboard aircraft. The U.S. Congress has taken strong steps to address cybersecurity needs for aviation, under the "FAA Extension, Safety, and Security Act of 2016." The law (P.L. 114-21 Sec. 2111. Aviation Cybersecurity) calls for a "comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the national airspace system, civil aviation, and agency information systems using a total systems approach."

Additionally, the Department of Homeland Security, Department of Defense, FAA, and the Federal Bureau of Investigation are collaborating to address cybersecurity issues. The Canada-U.S. Regulatory Cooperation Council included cybersecurity as one of its priorities, highlighting the need for joint planning and priority setting, collaborative research projects, information exchanges, and standards development to harmonize our mutual approaches to cybersecurity measures for all connected vehicles.

[3] "Managing Cybersecurity Risk in Weapon Systems" Dr. Raju Patel, Aircraft Systems Authorizing Official, US AIR FORCE, LCMC, March 21, 2017

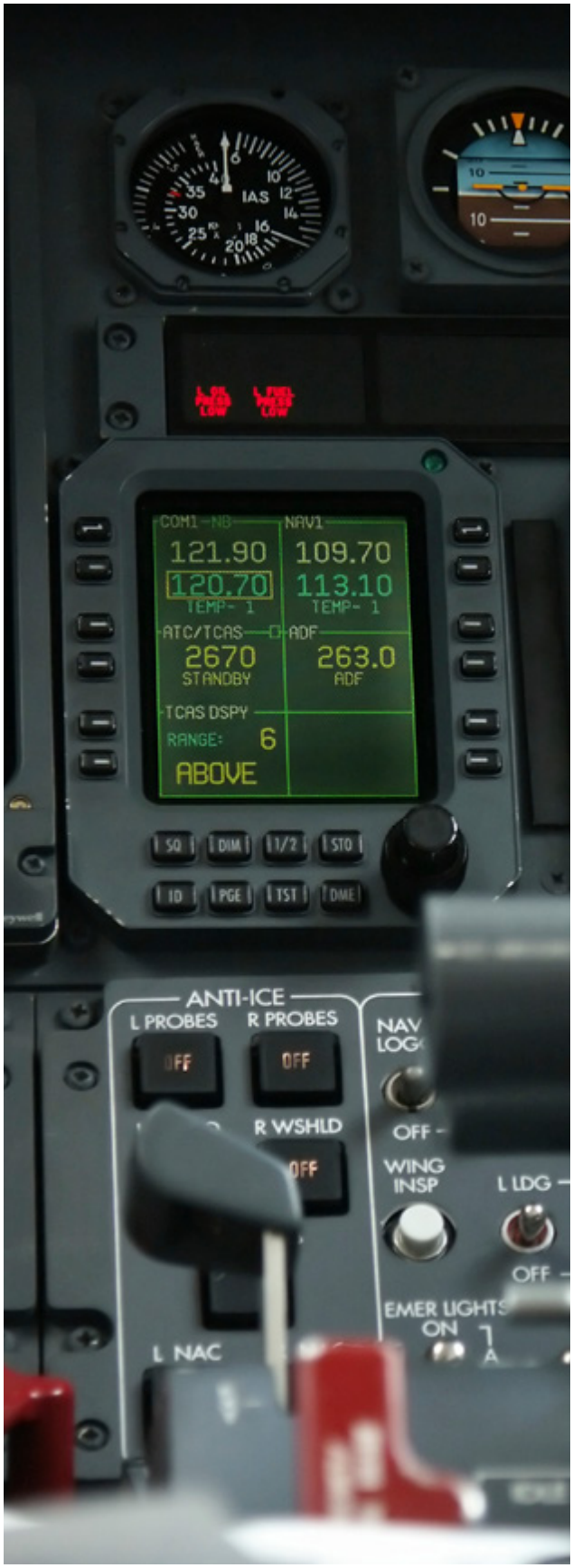


The Pilot's Role in Defending Against Cyber Attacks

Pilots are responsible for the safe and secure operation of flight. However, FAA aircraft airworthiness standards do not presently require that aircraft systems monitor, detect, or alert flight crews to the presence of a cyber attack. Further, flight crews generally do not have training, procedures, or technology to protect the aircraft from such operational threats. Depending on the nature of an inflight cyber attack, the flight crew might not be aware of it, and may not be prepared to counter it.

In recognition of this shortcoming, one manufacturer is working on a "research and development project that aims to provide commercial and military pilots with a cyber-attack warning system within the next year. The aerospace and defense manufacturer says two products are in development: a software-only technology and a hardware-deployable module. The software will provide a quick and easy fix should the need arise, while the hardware is designed to give operators a hard-wired solution capable of protecting critical aircraft systems from cyber attacks. [T]he team is developing software that looks for anomalies on aircraft data buses, remote terminals and any device that could be connected to the buses such as annunciators, flaps, lights and landing gear."

A well-trained and qualified professional pilot is a critical element for ensuring that aircraft security, and the associated mitigations described above can be deployed when a cyber threat is identified during flight. To maintain a strong cybersecurity posture for the safety and security of the flight, a comprehensive strategy that is consistent with the cybersecurity provisions of P.L. 114-21 and includes the critical role of the flight crew, is essential.



[4] http://www.aviationtoday.com/2016/12/29/raytheon-is-working-on-an-airplane-cyber-attack-warning-system/

Conclusions

- Government and industry are increasingly proactive and involved in establishing comprehensive cybersecurity strategies that include policies, rules, and mitigations to protect commercial aircraft from cyber attacks.

- Airline pilots have as their primary responsibility, and are the final authority of, their flight's safety and security, including as it relates to cyber attacks on the aircraft. Accordingly, pilots should be considered a fundamental resource when developing comprehensive strategies on how to mitigate inflight events.

- Command capabilities and functionalities for monitoring aircraft system health for potential cyber events, as well as the tools needed for the mitigation of real-time events, should be readily available to pilots on the flight deck. Cyber attack warning systems should be researched and developed for use by the flight crew on commercial aircraft.

Air Line Pilots Association, Int'l
1625 Massachusetts Ave., NW | Washington, DC 20036 | 703-481-4440
Media@alpa.org | www.alpa.org
June 2017