Aerospace Industries Association (AIA)
Air Line Pilots Association (ALPA)
Joint Recommendations for
Aviation Cybersecurity

AIA Civil Aviation Cybersecurity Subcommittee

AIA ALPA Cybersecurity Recommendations WG:

Ms. Siobvan Nyikos (Boeing Commercial Airplanes)

Dr. Stefan Schwindt (GE Aviation)

Mr. Patrick Morrissey (Collins)

Air Line Pilots Association, International:

First Officer Matt Clark (ALPA Aviation Security)[1]

First Officer Tom Merrill (ALPA Aviation Security)

First Officer Eric Hendrickson (ALPA Aviation Security)

Ed Hahn (ALPA Engineering & Air Safety)

Xylene Gonzalez-Pelayo (ALPA Engineering & Air Safety)

[1] Matt Clark is now working at Delta Airlines

Table of Contents

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

1 Introduction

"Proposal/Rationale for Flight Crew Alerting of Cyber Events That Affect Avionics Functions" was presented by Air Line Pilots Association, International (ALPA) in December 2019 in RTCA Special Committee 216, outlining concerns around aircraft cybersecurity[2] from the pilot's perspective. Since then, there have been updates in industry standards and regulations as well as more collaboration with other aviation ecosystem stakeholders. This paper outlines discussions starting in 2021 between pilots, represented by ALPA, and airplane and avionics system manufacturers, represented by the Aerospace Industries Association (AIA) Civil Aviation Cybersecurity Subcommittee. The paper summarizes topics which were covered in those discussions and the conclusions which were drawn. Many of the topics resulted in considerations for future research activities, design, and process updates. The focus of the discussions were cybersecurity risks, mitigations, and if/how pilots might need to be informed of or respond to these events. This in turn raised questions about how the pilot receives, interprets, and uses data from the modern connected aircraft. As with any potential safety impacting event on an aircraft, mitigations to prevent their occurrence can be technical (i.e., handled by the aircraft and its systems), procedural (i.e., requiring pilot notification, intervention, and training), and/or physical (e.g., cockpit security door).

For the pilot community, there is growing concern about how cyber threats[3] are managed within the aircraft and to what degree. Pilots need to have some understanding of how avionics systems operate and are interconnected to better understand what happens in abnormal situations, including situations caused by cyber. This would enable pilots to be better informed to compensate for failed components and ensure a safe completion of the flight. To support this operationally, pilots are often provided with redundant information from diverse sources to validate against each other. Additionally, they are provided real-time alerts which feed their situational awareness of the aircraft and its systems. This aggregation of information is used by the pilot to feed their mental model of the aircraft, its systems, surrounding aircraft and weather, and threats to those systems which might impact the flight. In the event of system failures, pilots are provided with Quick Reference Handbooks (QRHs) which provide procedures to follow that mitigate the effect of the failure and/or advise the pilot to land as soon as practicable. In this context, what cyber events might occur in an aircraft which could impact the safety of flight? What, if any, notification should be given to the pilot in these cases and what kind of procedure should they follow? Would the pilot react differently if the availability or integrity of a system was caused by a cyber event[4]? These questions and others were explored during these discussions, many of which are summarized in the following sections along with recommendations for future consideration.

[2] The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. *(44 U.S.C. Sec 3542)*

[3] For a definition of cyber threats see footnote for IUEI

[4] Also known as a "Security Event", an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant *(ISO 27001)*

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

2 Pilots' Perspective on Cyber Security

As part of the overall duties of the pilot in command, Title 14 of the Code of Federal Regulations (CFRs) 91.3 (Responsibility and authority of the Pilot in Command) states that "the pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft." Implicit in carrying out this responsibility is the pilot having knowledge of the condition of the aircraft.

For pilots, one of the biggest considerations is knowing when they can no longer trust a particular system or instrument. The training and procedures they are provided with are founded in the assumption that notifications and indications from the aircraft are correct. In most instances, aircraft system notifications to the pilots will only delineate whether a system is working normally or is inoperative. Only in rare situations is it acknowledged through instruments or indications/notifications, that a system might otherwise be adversely impacted, degraded, or is receiving bad data. Ultimately, if a system cannot be trusted and it cannot be cross checked against other systems and data sources, then there is the potential additional risk and issues which could compound into a more significant event.

When the safety analysis extends to include anomalies from intentional acts by unauthorized persons, the considerations for informing the pilots when a system can no longer be trusted gain additional importance. Therefore, pilots are advocating for the development of onboard functions which support real-time detection, mitigation, and pilot notification of cyber security events[5] that could affect safety of flight. It is acknowledged that this raises many issues for correctly identifying events, defining appropriate thresholds for alerts, and developing appropriate actions in response to these alerts.

It is important to note that if detection and notification capabilities are not developed or included, then pilots alone would become the de-facto means for identifying a cyber-related event or issue. Just as it has become unacceptable for pilots to engage in unstructured system troubleshooting of mechanical or systems failures, it is not a viable or prudent option to rely on pilots with varying levels of expertise to perform unstructured cybersecurity identification and mitigation. Instead, it would be much more beneficial to develop an approach that works within an existing framework for dealing with non-normal situations. Current training and standardization methods have been stalwarts of the high levels of safety in aviation and are rooted in aircraft systems performing monitoring, detection, and notification. It could be valuable to apply that approach when considering how pilots will or should respond to a security event.

3 Regulations for Cyber Evaluation for Safety

3.1 Safety Regulations

Air travel remains the safest form of transportation today in-part because of the incredibly high bar which has been set for quality in the design and operation of those systems. That bar is set through Title 14 of the Code of Federal Regulations which define requirements for the whole of the aviation system, from Airline operations and pilot procedures to design requirements. For system designers and suppliers, design

[5] Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

consideration for safety in Part 25 (Air Transport) operations is founded in Federal Aviation Regulation (FAR) 25.1309 (Equipment, Systems, and Installations) which reads as follows:

> ***§ 25.1309 Equipment, systems, and installations.***
>
> ***(a)*** *The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.*
>
> ***(b)*** *The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that -*
>
> ***(1)*** *The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and*
>
> ***(2)*** *The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.*

This regulation makes clear that all potential impacts to safety, regardless of source, must be accounted for in the design of the aircraft and its supporting systems. The definition of potential impacts to safety in this definition is not bounded. They could be sourced in mechanical or hardware failures, environmental causes (like lightning), or for the purposes of this whitepaper, software defects or vulnerabilities (introduced in design, or implementation). This has far-reaching implications for suppliers for the aviation industry as it requires every system and component to be evaluated in the context of safety to ensure it does not contribute to a safety event. Where risks are identified in a system design, they must be mitigated.

Achieving this lofty goal occurs through the application of a rigorous design process which is guided by a number of standards and specifications. These specifications are called out through FAA Advisory Circular 25.1309-1A (System Design and Analysis) as an acceptable means of compliance. A few of these are as follows:

- SAE ARP4754: Certifications Considerations for Highly Integrated or Complex Aircraft Systems
- RTCA DO-178C/EUROCAE ED-12C Software Considerations in Airborne Systems and Equipment Certification
- RTCA DO-254/EUROCAE ED-80 Design Assurance Guidance for Airborne Electronic Hardware

These documents recognize varying assurance levels of systems in the aircraft in the context of safety to ensure the systems (as designed and developed) can meet the originating regulation. These levels are named simply A through E with A (adequate assurance mitigating catastrophic impacts) being the most critical (i.e., poses the most risk to the safety of continued operation) and E (no safety effect) being the least risk generally only showing the system performs its intended function and does not physically combust (i.e., burn).

To eliminate defects which might occur in design and implementation, systems fulfilling roles at increasing safety levels must have higher degrees of traceability between requirements, implementation, and verification. At level A all requirements must trace through multiple levels down to each line of code which then must be traced to the tests which verify the function of that line of code to eliminate potential design and implementation defects. This equates to every line of code being tested for both function and failure in safety critical systems. This safety-first design and development process followed by the aerospace industry has resulted in a safety record that cannot be paralleled in any other transportation industry.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

3.2 Security Regulations

While this provided a good foundation and created highly robust systems, FAR 25.1309 did not consider adverse events from intentional acts. As a result, it became apparent that a specific rule for cyber was needed and an accompanying process to identify those attack paths. So, in 2014-2016 a Federal Aviation Administration (FAA) Aviation Rule Advisory Committee (ARAC) on Aircraft System Information Security Protection (ASISP) was formed to provide a rule update recommendation. As an outcome, in 2020, the European Union Aviation Safety Agency (EASA) added 25.1319 in amendment 25 (the FAA will be adding a parallel version in 2023/2024):

(a) "Equipment, systems, and network information protection (a) Aeroplane equipment, systems, and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEI)[6] that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed, and mitigated as necessary

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA)[7] available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained."

The wording is purposefully specific that cyber security events (IUEI) which could impact safety must be identified, assessed, and mitigated. It makes clear that for certification of transport aircraft, security must be considered as part of the safety analysis. Further, in part B, it clarifies that any instructions required for the airlines or pilots to take to maintain airworthiness must be provided as part of the ICA. In effect, to meet this requirement, any procedures which need to be carried out by airline personnel such as maintainers or pilots to support continued airworthiness must be provided.

In support of this requirement, systems which host cybersecurity functions provide event detection related to those functions. These events are then evaluated in the system safety context for the level of system impact of the occurrence which is then elevated to the correct level of alerting based on the defined impact. In most systems to date these events are logged for maintenance review with instructions provided as part of ICA per the safety analysis. If the event is generated by the security function, as defined in DO-326A/ED-202A Airworthiness Security Process Specification, specific requirements are levied to ensure the event is tagged appropriately as security related and a review cycle defined.

The above rule for cyber security is supported by the two cybersecurity standards DO-326A/ED-202A and DO-356A/ED-203A Airworthiness Security Methods and Considerations. The first, as mentioned previously, is a process specification; the second provides activities, objectives, and methods in support of the process

[6] A circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming. *(DO-356A: Section 2.1.1)*

[7] The instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which are required in accordance with the applicable Certification Basis or Standard to be developed and/or referenced by the Design Approval Holder. *(EASA CM No.: CM–ICA-001 Issue 01 issued 02 May 2017, Section 1.4)*

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

specification. Additionally, it provides alignment between many of the defined objectives to objectives called out in other standards which can also be used to fulfill those listed in DO-356A.

3.3 Logging and Alerting

Generally, when faults occur on an aircraft, the aircraft and crew are guided to react dependent on the defined criticality of the issue and associated scenario. The two main options are logging a fault or providing an alert.

There are multiple logs maintained onboard an aircraft. Airborne systems will have an internal log for fault conditions local to a device. Additionally, most commercial aircraft typically have a central maintenance system which collects and aggregates fault messages from all onboard systems for retrieval by pilots and maintenance personnel in a central location. Where knowledge of aircraft behavior is necessary for post-accident investigation, certain parameters and fault codes are sent to the Flight Data Recorder to provide a protected storage of the most recent hours of flight. To support monitoring of anomalies in pilot performance and to aid investigation of minor incidents, parameters and fault codes are sent to the Quick Access Recorder which allows easy access to these logs.

Crew alerting onboard the aircraft is a safety driven process starting with a Functional Hazard Analysis from which the failure conditions related to aircraft functions are identified. SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, suggests crew alerting to be identified as interfacing functions. In determining the severity and acceptability of a failure condition, the ability to alert on and react to the failure condition is considered. For all aircraft functions, the alerts for functional failures are tabulated and ranked in terms of their severity (Warnings, Cautions, and Advisories) and allowable reaction times (e.g., failures which require a response within 30 seconds are prioritized over failures with an allowable response of 5 minutes). For each failure, a suitable message to be displayed on the alerting console is chosen and suitable additional alerts are defined, these include tactile feedback such as stick shaker, aural indications including annunciation, and visual indications including various forms of lights. Simultaneously, the necessary manuals are written to provide actionable guidance for the alerts, definitions of Memory Items, Quick Reference Handbook procedures and Flight Crew Operating Manual abnormal procedures. As the technical design is defined and implemented, human factors assessments are made to ensure the chosen concept is appropriate for the task, is clear, unambiguous, and minimizes the potential for flight crew errors. Evaluations and assessments are performed by analysis, in simulators, and during flight testing to validate and verify that flight crew responses are as expected to address the failure conditions. In short, any information provided to the pilots must be usable and actionable (and not create unnecessary distractions).

The design of crew alerting for Part 25 is driven by the regulations in 14 CFR 25.1322 Flightcrew Alerting, and the associated Advisory Circular 25.1322-1 Flightcrew Alerting Documentation Information. The regulation requires alerting to be appropriate for the condition the aircraft is in and to consider human factors in perceiving and acting upon an alert. The aircraft must inform the pilot of any non-normal operations or conditions and necessary actions to be taken and the alerting must be suitable to ensure that the flight crew are able to understand the message under any foreseeable conditions – e.g., lighting conditions, stress, and multiple simultaneous alerts. Alerts also need to be removed for transient conditions to ensure inappropriate actions are not taken on account of outdated information. The regulation provides a hierarchy of alert types:

- Warning: Conditions that require immediate awareness and immediate response
- Caution: Conditions that require immediate awareness and subsequent response

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

- Advisory: Conditions that require awareness and may require a response

Warning and caution alerts are prioritized and attention getting cues are provided by at least two different senses out of aural, visual, or tactile.

The Advisory Circular AC 25.1322-1 provides further guidance on ensuring human factors are considered during the development of alerting, including the colors used, managing alerts to ensure situational awareness is maintained and prevent overload of the flight crew, choosing alert sensory types. Additional Advisory Circulars related to alerting provide guidance on the instruments providing alerts in the cockpit and the safety of aircraft functions and systems requiring alerting.

In the security standard DO-356A/ED-203A Airworthiness Security Methods and Considerations section 6.1.1, the link between security events and safety alerting is established. "Security events that cause a safety effect should alert flight crews in accordance with guidance provided by AC 25.1322-1 and related documents. If a security event or malfunction occur, the flight crew should be alerted to the safety effect and should be made aware of what resources and/or assets remain to maintain the safety of flight." This ensures that any security event which could result in a safety effect must follow the safety process consistent with all other failures to assure the correct level of logging or alerting is raised.

4 Aircraft RF Interfaces and Systems

In large, most aircraft systems are insulated from the attack surface[8]. But there are many which are necessarily exposed for their function. This includes communications, navigation, and surveillance systems all of which receive external signals and translate them into data which may be used by the pilot or other onboard systems for decision making. Many of these systems include redundancy through other functions or systems to support detection and investigation of anomalies.

DO-326A/ED-202A does not seek to provide guidance for specific systems as it's a process specification. In 2016, RTCA updated the Minimum Operational Performance Standards (MOPS) Drafting Guide to include a definition of cybersecurity risks in any updated MOPS. This helps ensure as functional performance specifications are created or revisited for functions on the aircraft, they will document risks which need mitigation by the system designer in future versions.

The following sections discuss some of the more exposed systems.

4.1 Navigation

The aircraft is supported by a multitude of navigation systems and sources, some stand-alone (e.g. inertial reference systems, radar altimeters) and others dependent on external signals (e.g. global navigation satellite systems and ground based navaids), to support redundancy as well as providing access to different types of navigational routes and approaches.

[8] A term for the parts of a system which are exposed to a possible attack. It is comprised of the untrusted interfaces in an operational system.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

4.1.1 Global Navigation Satellite System (GNSS)

GNSS is the broader term for the set of systems more commonly referred to in the U.S. as Global Positioning Systems (GPS). There are five GNSS satellite constellations available for navigation around the world: GPS (US), QZSS (Japan), BEIDOU (China), Galileo (EU) and GLONASS (Russia). The technology has become the most commonly used form of navigation in aviation due to its global reception, high reliability and accuracy. But in recent years there has been a lot of discussion regarding the integrity of those signals and if they can be jammed or spoofed. In 2016, a study was conducted by EASA to evaluate the susceptibility of GNSS to cyber events and associated pilot reactions. The results of the study can be found here. This has raised the point that the industry has become overly reliant on legacy GPS systems.

In response, the GNSS receiver standardization team (RTCA SC-159/ EUROCAE WG-62) is currently working to define requirements for spoofer detection in the next DFMC (Dual Frequency Multi-Constellation) SBAS (Satellite-Based Augmentation System) capable receiver standard (ED-259). The next version of this standard defines 7 classes of spoofers in appendix A, with classes 1-4 being mandatory for remediation and classes 5-7 as optional.

4.1.2 Ground Based Navigational Aids and Landing Systems

Instrument Landing System (ILS), VHF Omni-Directional Range (VOR), Distance Measuring Equipment (DME), and self-contained on-board systems, such as Inertial Reference Systems (IRS) pre-date GNSS by decades and served as the basis of nearly all aviation navigation prior to the advent of GNSS. Navigational aids are similar to GNSS in as they operate utilizing signals broadcast from fixed ground stations opening them up to jamming and spoofing vulnerabilities like GNSS. The broadcast signatures are interpreted by systems on the aircraft to aid in determining the aircraft's navigation position. Being much older than GNSS, these signals aren't terribly difficult to spoof, but due to their dispersed nature offer some robustness against spoofing.

While these systems are less accurate than GPS it should be noted that the two can serve to benefit each other for security. The majority of aircraft today navigate via a specific Performance-Based Navigation (PBN) specification (Nav Spec). Most PBN Nav Specs require GPS as the primary means of the aircraft's navigation eligibility to conduct PBN operations. Modern PBN Nav Specs require navigation and GPS integrity monitoring, but they remain vulnerable to GNSS jamming and spoofing. Navigational aids and on-board systems like VORs, DMEs and IRS offer a means to mitigate jamming and spoofing, however, there are still many vulnerabilities that need to be addressed.

4.1.3 Radar Altimeters

Radar Altimeters provide valuable input to the system on altitude over ground during approach operations and have gained much attention over the last year in the US due to unintentional 5G interference concerns. Working groups SC-239 and WG-119 from RTCA and EUROCAE have been working proactively to address cybersecurity considerations for spoofers and jammers within Subgroup 6 in the planned MOPS update. The urgency of short-term activities around 5G interference has delayed some of this effort but it is still on the roadmap for the next release of the document which is anticipated at the end of 2023.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

4.2 Communications

4.2.1 Voice

Aviation communications have long been a subject of research and speculation for the risk they pose. Aviation voice communications are in the clear (unencrypted) and follow a party-line design such that anyone in the broadcast range of the transmitter on the correct frequency can hear the transmission. Likewise, anyone can transmit on those same frequencies. But while at first look the design seems risky, there are mitigations present in the current system. The party-line design of voice communication provides a layer of security similar to intrusion detection systems (IDS) in a network. All the pilots listening on a frequency mentally process the radio calls for their own situational awareness but in doing so they are also listening for errors or anomalies within the system. Interestingly, with voice communication, the listener consumes both the content of the message but also potentially a recognition of the voice of the sender. Discussions with professional pilots have revealed that they recognize many of their ATC counterparts by voice and understand their communication style. These elements of a voice fingerprint provide a certain level of validation of the other side of the communication. Also, radio communication protocols between pilots and controllers follow a call, acknowledgement, readback, acknowledgement progression. This is to ensure instructions given to any pilot were correctly received and understood. So, if an independent broadcaster were to give an instruction which was inconsistent with that of ATC, there are three potential points of detection: voice signature of the broadcast, the readback of instructions, and passive listeners in this network.

4.2.2 Datalink

Datalink communications, on the other hand, do not benefit from the party-line design and might be more at risk from an independent broadcast. However, doing so is more complicated than the voice scenario where the attacker just activates a microphone and speaks. The data exchange between air and ground must follow a predictable sequence, and data packets must be wrapped with the correct headers and sequence numbers for messages to be received and presented to the pilot.

The good news for point-to-point communications, like Datalink, is the evolution toward the next generation Internet Protocol Suite (IPS) service for Aeronautical Safety Services (ARINC 658) which will provide secure datalink messaging capability between the aircraft at the ground. Until IPS becomes more widely available, pilots should be mindful of messages received over datalink to ensure they are consistent with the expected progression of flight. If there is doubt about a received message or direction, it is recommended the information be confirmed over a voice channel. Pilots have resources available to check the integrity of the information they receive for navigation, surveillance, and communications (voice and data). Per DO-350A, Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard), 2 out of 3 of these must be wrong or unavailable to be hazardous. While the likelihood of a coordinated attack to do this is very low, aviation cyber stakeholders should continue to explore mitigations to ensure the risks are adequately mitigated.

4.3 Surveillance

ADS-B (Automatic Dependent Surveillance-Broadcast) was developed to enable shared situational awareness amongst controllers and pilots to have a better understanding where aircraft are within the airspace system. Since the protocol it utilizes has no integrity protections, ADS-B input cannot be used alone for safety critical decision making. Applications like CAVS (Cockpit Display of Traffic Information (CDTI) Assisted Visual

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

Separation) require verification of ADS-B information by pilot visual contact with the traffic. Other systems such as TCAS (Traffic Collision Avoidance System) or ACAS (Aircraft Collision Avoidance System) require a position validation through transponder interrogation and reply before a safety maneuver (Resolution Advisory) can be issued.

While there is no work planned at this time to update the protocol, new protocols with better integrity features are being developed to support operations in higher density airspace environments like those envisioned for Urban Air Mobility (UAM).

5 Recommendations and Research Opportunities

From the discussions described above, the AIA Civil Aviation Cybersecurity Subcommittee and ALPA representatives have developed the below agreed upon recommendations for industry to consider and pursue.

5.1 Training

Throughout this paper it has been noted that the current system includes many human detectors currently operating as part of the aviation system today. These include pilots and controllers who have the greatest access to real-time data within the system. In their current roles they serve as the first line of detection when non-normal conditions exist. While experience with independent broadcasters of voice traffic is well established, less experience exists with independent broadcast of navigation signals. Research should be conducted into the tactics, techniques, and procedures (TTPs) which are employed by crews in the presence of navigation anomalies and their effectiveness in identifying and mitigating the anomaly.

5.2 Design & Testing

In cybersecurity maintaining data integrity is key to success. Cyber events occur in the processing of data which is received from outside the system boundary. System integrators need to be focused on this aspect as they architect and design systems. Data received from outside the system needs to be identified in the design and flowed down to system developers and suppliers so they can ensure the subsystems and components are robust to handle the conditions when the data might be spoofed, jammed, or otherwise altered. This approach is defined in DO-326A/ED-202A and the methodology companion document DO-356A/ED-203A. OEMs and TC holders need to be sure they are testing a full complement of functional security and robustness scenarios. Including at the aircraft level, to ensure the final set of pilot procedures and system responses are complete in addressing scenarios which could be presented to the pilot in operation. If a GNSS signal is spoofed how does the complete system respond? Are other systems affected by the change in time that occurs during GNSS spoofing and how should the pilot respond to that condition? Incorporating pilots of varying experience levels into these testing scenarios becomes tantamount in ensuring the system mitigations are at the correct level.

Industry needs to continue to pursue advanced integrity features for airborne systems to ensure the integrity of those systems as they are updated in the field and move through repair and replacement cycles. While consumer grade technologies exist for this capability it has drawbacks for use in airborne safety critical systems, such as restart times which are increased when cryptographic functions are introduced into the restart cycle. Technologies like attestation should be further explored to provide cryptographic strength in integrity monitoring without the drawbacks of relying on consumer technology.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org

5.3 Research into Non-normal Operations and Navigation

More research should be conducted to assess pilot and system responses to the manipulation of input data to the aircraft. The outcomes of this research could serve to enhance aircraft systems currently under development or those of the future through updates to MOPS (Minimum Operational Performance Specifications). It would also provide insight into how intentional actions by malicious actors might attempt to change the situational awareness of a flight crew and if there is a need to evaluate existing flight crew TTPs for safety impacts. Aviation industry cyber SME's should establish research requirements to include scenarios, information and parameters to be manipulated for TTP research evaluations. Industry provided scenarios could be established to drive the research to enable relevant and realistic research outcomes which could refine future performance testing as well as crew TTPs.

The FMS/APFD (Auto Pilot Flight Management and Flight Director Systems) are the center of all navigation operations in a complex aircraft. It serves as the authority on the position of the aircraft to the rest of the system defining the plan for staying on course or returning to course if a deviation is detected. These systems need to be resilient to the potential loss or obfuscation of GNSS and utilize integrated logic which compares a variety of navigational inputs (GNSS, inertial, VOR, DME, and ranging information from other future sources (LDACS, 5G, etc.)). This approach would increase technical diversity in location resolution, thereby increasing the difficulty in spoofing an aircraft's location via jamming a singular signal.

5.4 Updates to Guidance

Current regulations call for security operational procedures to be flowed down through ICA. AMC 20-42 lists ICA but makes no reference to physical and operational security measures. This means that there may be a gap in guidance for operations within the AFM (Aircraft Flight Manual), Engine Manual, FCOM/AOM (Flight Crew/Aircraft Operating Manual) or AMM (Aircraft Maintenance Manual). Further review should be conducted to identify if these documents should get updated per current regulations, if further guidance is required, or if current guidance is adequate and needs better interpretation.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928
703.358.1000 | www.aia-aerospace.org

Air Line Pilots Association, Intl
7950 Jones Branch Drive, Suite 400S | Mclean, VA
703-481-4440 | www.alpa.org