Aviation Cyber Security Efforts

Airlines Electronic Engineering Committee (AEEC)

Rev version H: May 2018
Paul J. Prisaznuk
AEEC Executive Secretary and Program Director

This document summarizes the efforts and products of ARINC Industry Activities and the Airlines Electronic Engineering Committee (AEEC) in the areas of aviation cyber security. It discusses how the overall subject of cyber security is treated within the context of ARINC Standards.

Every ARINC Standard is prepared with aviation cyber security in mind. This starts with the objective to discuss the role that cyber security might play in the respective system definition, functional definition, equipment definition, and so forth. Each standard may define system-specific cyber security guidelines or it may invoke general guidance found in existing ARINC Standards described later in this report.

ARINC Industry Activities cyber security efforts are focused within the Airlines Electronic Engineering Committee (AEEC) responsible for roughly 300 ARINC Standards, including 50 new ARINC Standards being produced by 25 AEEC Subcommittee activities responsible for Communication, Navigation, Surveillance, Cabin, and other related avionics disciplines. Much of the cyber security effort is directly influenced by data communications and the evolution of new systems, namely those using the Internet Protocol Suite (IPS).

From the earliest of times, ARINC Standards have acknowledged the possibility of digital data being corrupted in a way that could lead to hazardous and misleading information. Some early examples to ensure data integrity are as follows:

- Parity Checking (ARINC 429 Data Bus – 1977)
- Cyclic Redundancy Checking (CRC) (ARINC 629 Data Bus – 1989)
- Domain Separation (ARINC 664 Network Bus – 2002)

These data bus standards are used extensively on nearly all commercial aircraft in service today. They provide some degree of isolation and protection of sensitive avionics equipment. These data bus standards are being used to create avionics systems architectures that connect trusted equipment and at the same time they isolate and segregate other systems that may be open to undesirable communication paths. The implementation of robust avionics architectures is the primary means to protect the aircraft control domain.

ARINC Report 811: *Commercial Aircraft Information Security Concepts of Operation and Process Framework* was published on December 20, 2005. The goal is as follows:

> "*The project will develop a Concept of Operation for a common security framework and a set of common security mechanisms which, when designed and implemented, will not impair the ability to safely fly and dispatch aircraft in a timely manner.*"
>
> ARINC 811 facilitates an understanding of aircraft information security and to develop aircraft information security operational concepts. This common understanding is important since a number of parties within the aeronautical industry are considering aircraft information security.
>
> ARINC 811 also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.
>
> ARINC 811 does not attempt to solve specific application, communication, or network security issues, but provides a concept of airline operations and process framework to the airlines, airframe manufacturers, avionic suppliers and other stakeholders.
>
> This document includes a common set of terms and concepts, bridging between airline organizations and the terrestrial network security industry.

ARINC has also published a **Technical Application Bulletin**, *Considerations for the incorporation of Cyber Security in the Development of industry Standards* (AEEC Letter 12-180/ABN-35A dated October 24, 2012.)

> The purpose of this document is to provide information to system engineers preparing industry standards for networked systems to ensure that appropriate cyber security provisions are included in emerging systems. The following are recommended:
>
> - Security issues that affect avionics, associated cockpit systems, and cabin systems should be considered thoroughly by those developing standards.
> - Company representatives participating in standards development activities should communicate with their in-house security specialists.
> - New standards development activities should address how cyber security and common security solutions will be considered.
> - ARINC Report 811 and this document should be used by those developing standards to address airline security needs.

ARINC Standards for Aviation Systems

The majority of ARINC Standards define larger systems that will be implemented as communication systems, navigation systems, surveillance systems that may require a standardized mix of hardware and software functions subject to cyber security standards.

ARINC Report 658: *Internet Protocol Suite (IPS) for Aeronautical Safety Services – Roadmap Document,* published December 2017.

> In 2015, the AEEC Executive Committee formed the Internet Protocol Suite (IPS) Subcommittee to develop a roadmap for the introduction of an Internet Protocol Suite for Aeronautical Safety Services. Airbus and Boeing lead the effort on behalf of their airline customers. ARINC Report 658, a program plan, cites the role of cyber security, the role of providers, and the role of stakeholders, etc. This document sets the expectations for cyber security expectations in aviation. Follow-up work is being planned for 2018 and beyond.

ARINC Project Paper 858: *Internet Protocol Suite (IPS) for Aeronautical Safety Services - Technical Requirements [draft working title]*

> ARINC Project Paper 658 is expected to define protocols, architectures, and domains as well as specific security requirements using IPv6. This document is expected to provide cyber security guidelines applicable to aviation as a whole, both air and ground.

ARINC Characteristic 771: *Low-Earth Orbiting Aviation Satellite Communication System*, includes security considerations. The document was adopted in April 2016 and is now published as an ARINC Standard. Supplement 1 was approved in April 2018.

> **Section 4**, *Security Considerations*, outlines objectives, architecture, security analysis, and multiple transceiver design for physical separation.

ARINC Characteristic 781: *Mark 3 Aviation Satellite Communication Systems* was first published October 4, 2005. Supplement 7 was published in August 2017. This document includes a definition of the Inmarsat SwiftBroadband (SBB) Security Overlay as it will be implemented in commercial service.

Security considerations were addressed in this document from the beginning and will continue to evolve as needed. Particular areas of standardization are:

> **Section 3.4.3,** *Security,* provides a short overview of security as it relates to this document and recommends that **EUROCAE ED-202/RTCA DO-326:** *Airworthiness Security Process Specification* be used as the basis of the security process.
>
> **Attachment 8,** *Network Security for SwiftBroadband (SBB) Safety Services,* includes guidance on security considerations for SBB safety service terminals including the type of segregation that is expected to be acceptable to regulatory authorities and airframe manufacturers for such terminals. Supplement 7 introduced a VPN between the ground and the aircraft to secure the ACARS service.

Appendix B, *Security Analysis of the SATCOM Ethernet Interface*, provides a security analysis of the Ethernet Interface defined in Attachment 5. Appendix B includes design principles for secure airborne networks, analysis methodology, and security analysis of Satcom Interfaces.

ARINC Characteristic 791: *Mark I Aviation KU-Band Satellite Communications System, Part 2, Electrical Interfaces and Functional Equipment Description* was first published July 2, 2013 and more recently Supplement 1 was published July 28, 2014. An updated version of this document is in-work and expected to emerge as a mature document in 2018. Cyber security guidelines will be revised for currency and applicability.

Security was addressed in these documents from the beginning and will continue to evolve as needed. Particular areas of standardization are addressed in:

Section 2.5, *Network Security*, provides a short overview of security as it relates to this document and an Ethernet Domain Schematic. This section notes that ARINC Characteristic 781 provides a baseline analysis for a similar satcom system and that network security features assuming ARINC 781 security analysis is provided in Section 5 and Appendix A.

Section 5.0, *Security*, provides an introduction and addresses the following: plan for mitigation criteria, impersonation, malicious software, denial of service, implementation of functional segregation, control partition, operational partition, interface partition, security objectives, and summary.

Appendix A, *Security Analysis of the Satcom Ethernet Interface*, provides guidance and references ARINC 781 Appendix B

Appendix H, *Security and Safety Services*, notes that an ARINC 791 Satellite Communication System is licensed on a secondary basis for non-safety correspondence. There is no expectation that ITU will revise this status in the foreseeable future. There is no current basis to use Ku-band or Ka-band satcom for services wherein its loss or malfunction has an impact to the safe operation of an airplane. However, issues which need to be addressed for such systems to be approved for safety services are included.

ARINC Specification 822A: *On-Ground Aircraft Wireless Communication* was adopted in April 2016 and published in July 2016.

The document provides cyber security guidelines for the use of commercial data links connected while the aircraft is located on the ground. These include IEEE 802 series and cellular telephony. This document is considered mature. Industry will be implementing the recommendations provided for in this ARINC Standard.

ARINC Specification 823, *DataLink Security, Part 1, ACARS Message Security* was published December 10, 2007. The purpose and scope of the document are as follows:

The purpose of ARINC 823 Part 1 is to provide an industry standard for ACARS Message Security (AMS), which permits ACARS datalink messages to be exchanged between aircraft and ground systems in a secure, authenticated manner using a uniform security framework. The security framework described herein is based on open international standards that are adapted to the ACARS datalink communications environment.

ARINC 823 Part 1, ACARS Message Security, sets forth the provisions available to airlines and Datalink Service Providers (DSPs) to protect ACARS messages that are exchanged over traditional ACARS air-ground datalinks (VHF, HF, and SATCOM) and ground-ground communication networks.

ARINC Specification 823, *DataLink Security, Part 2, Key Management* was published March 10, 2008. The purpose and scope of the document are as follows

The purpose of ARINC 823 Part 2 is to provide recommended guidance and provisions for ACARS Message Security (AMS) key management. The key management framework described herein is based on open international standards that are adapted to the ACARS datalink communications environment.

ARINC 823 Part 2 sets forth the guidance and provisions available to airlines and datalink service providers for the life-cycle management of the cryptographic keys that are necessary for proper and secure operation of ACARS Message Security. The security provisions contained in Part 1 of this specification supports the use of either public/private (i.e., asymmetric) keys or a shared secret (i.e., symmetric) key for secure session initiation and key establishment between communicating peer aircraft and ground entities. This document provides guidance and provisions appropriate for the life-cycle key management of each approach.

ARINC Report 835: *Guidance for Security of Loadable Software Parts Using Digital Signatures* was first published November 23, 2011. Supplement 1 was published January 2, 2014.

Airlines place a high value on aircraft information security. This document provides background and detailed technical information on existing methods to secure loadable software parts. A user should be able to implement their own tools and processes associated with these security methods if desired.

Section 3.0 Software Security

Section 4.0 Security Process (Airbus Aircraft)

Section 5.0 Security Process (Boeing Aircraft)

ARINC Report 842: *Guidance for Usage of Digital Certificates* was first published June 11, 2012. ARINC 842 is the aircraft-specific companion document to ATA Spec. 42 document, which specifies a digital identity management framework and standard digital certificate profiles recommended for use across the air transport industry. Supplement 2 was published July 2018. This update will ensure currency and applicability of cyber security guidance provided in ATA Spec. 42.

The purpose of this document is to provide guidance for key life-cycle management, which refers to the phases through which digital certificates and associated cryptographic keys progress, from creation through usage to retirement.

The guidance is based on open international standards that are adapted to the aviation environment, recognizing that a typical commercial airplane has a long lifespan, its operational environment is highly complex and regulated, and multiple stakeholders operate ground-based systems that communicate with airplanes. Using a standardized and consistent key management

approach, as proposed in this document, helps to reduce cost of design, implementation, and operation even across a heterogeneous fleet.

ARINC Report 852: *Guidance for Security Event Logging in an IP Environment*, published June 2017.

ARINC 852 sets forth guidance for IP-based onboard networks and systems residing in the Airline Information Services (AIS) and Passenger Information and Entertainment Services (PIES) domains by establishing a common set of security related data elements and formats that are produced by aircraft systems, suitable for use by airline IT and/or avionic supplier analytical ground tools. ARINC 852 assists in tracing and isolating cyber security events.

THE EFB USERS FORUM

The AEEC Executive Committee formed the Electronic Flight Bag (EFB) Users Forum in 2009 to discusses a wide array of EFB installation issues, connectivity issues, and cyber security. Delta Air Lines hosted the first meeting in April 2010. Semi-annual industry meetings welcome over 300 specialists.

Cyber security is on on-going discussion in the EFB Users Forum in the context of "the connected aircraft". This forum shares best practices widely used in enterprise-level computing, ecommerce and the like. These practices are shared within industry and applied to many aircraft installations.

SUMMARY

ARINC Standards incorporate security concepts from an aviation and airline perspective and often refer to and build upon other security related documents from other organizations:

- American National Standards Institute (ANSI)
- Air Transport Association (ATA)
- Certipath
- EUROCAE
- International Civil Aviation Organization (ICAO)
- International Standards Organization and International Electro-technical Commission (ISO/IEC)
- International Telecommunications Union (ITU)
- Internet Engineering Task Force (IETF)
- RSA Laboratories
- RTCA
- US Federal Public Key Infrastructure Policy Authority
- US General Services Administration (GSA)
- US National Institute of Standards and Technology (NIST)
- World Wide Web Consortium (W3C)

ARINC Standards represent a broad range of installed systems used in commercial service. Our cyber security initiatives have produced both general purpose guidance and specific guidance. Our cyber security focus has been on specific communication end-systems, for example, VHF datalink, Inmarsat SwiftBroadband, Iridium Satcom, and various L-Band and Ku/Ka Band systems defined by the respective ARINC Standards.

As aircraft become nodes within the airlines' enterprise network this magnifies the importance of cyber security for both the safety of the airplanes and for protection of the overall business operation. The communication needs of the airline business operations are, and must remain, separate from operational safety and air traffic communications. And given the "end-to-end" nature of cyber security, it is necessary for industry to consider cyber security provisions in the airborne systems and also in all the ground systems manipulating airplane data.

ARINC Industry Activities benefits from the many members and specialists represented on international industry groups (e.g., RTCA SC-216 and EUROCAE WG-72), which allows us to monitor and anticipate evolving procedural changes or new regulatory guidance. ARINC Standards are influenced by regulatory efforts, for example, special conditions imposed by FAA and EASA during the certification of new "e-enabled" aircraft, i.e., Airbus A350 and Boeing 787.

ARINC's cyber security guidelines are coordinated with many international standards bodies to ensure consistent guidance is provided to industry to minimize any overlap between standards and to ensure there is no contradiction among cyber security standards.

ARINC Industry Activities and the airline community through the AEEC are committed to ensuring that the ARINC Standards represent the airline user community needs for standardization in the area of aviation cyber security. Any party may raise a proposal to initiate a new ARINC Standard or to update an existing ARINC Standard. All such proposals are considered by the AEEC Executive Committee and appropriate action is taken.

Over 100 ARINC Standards make specific reference to aviation security requirements, in some cases physical security and in some cases cyber security. ARINC Standards can be found at http://www.aviation-ia.com/cf/store/documentlist.cfm

For more information, contact:

Paul J. Prisaznuk
AEEC Executive Secretary and Program Director
pjp@sae-itc.org