Civil Aviation Software Cybersecurity Recommendations

AIA Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – WG Chair (GE Aviation)

Sean Sullivan – WG Vice Chair (The Boeing Company)

Working Group Membership:

Ruchik Amin	GE Aviation
Todd Gould	Boeing
Stefan Schwindt	GE Aviation

Summary

Efforts to enhance secure software distribution and secure software loading practices throughout aviation ecosystem are ongoing. Significant strides have been taken in establishing standards and various implementation methodologies have been provided to the industry to help advance secure software distribution and loading in the aviation domain.

This paper seeks to provide guidance for compliance to new aviation standards and provides recommendations to standardize best practices as much as possible. This guidance complements the 2020 software recommendation paper establishing the basis for ARINC 645-1 secure dataloaders and provides proposals for transitioning civil aviation to secure software distribution for all aircraft. Suggested timeframes for adhering to each phase are also provided.

Table of Contents

Table of Figures

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

1 Aircraft Software Security Case

1.1 Problem Statement & Scope

Software – including the firmware code for programmable hardware as well as aviation databases – is critical for the safe execution of the complex electronics guiding and operating civil aircraft. As complex electronics are now ubiquitous on aircraft and increasingly no longer have mechanical backup, tampered software poses risks ranging from aviation safety to global aviation impact. This paper focuses on providing recommendations for securing software distribution and software loading onto aircraft Line Replaceable Units (LRUs) and Integrated Modular Avionics (IMA).

The lifecycle environment of software in aviation is complex as SW may pass through many intermediate steps and take alternative paths until it reaches its ultimate destination of installation on the aircraft. Figure 1 below provides a simplified illustration of the delivery paths and resting locations of software. The figure shows the flow of software as well as the physical hardware.

Due to the membership of AIA, the recommendations in this report apply to aircraft certified under Part 25/CS-25, Part 29/CS-29, Part 33/CS-E and Part 35/CS-P. These recommendations may apply to aircraft and parts certified under other sections; however, this requires endorsement by the appropriate industry organizations.

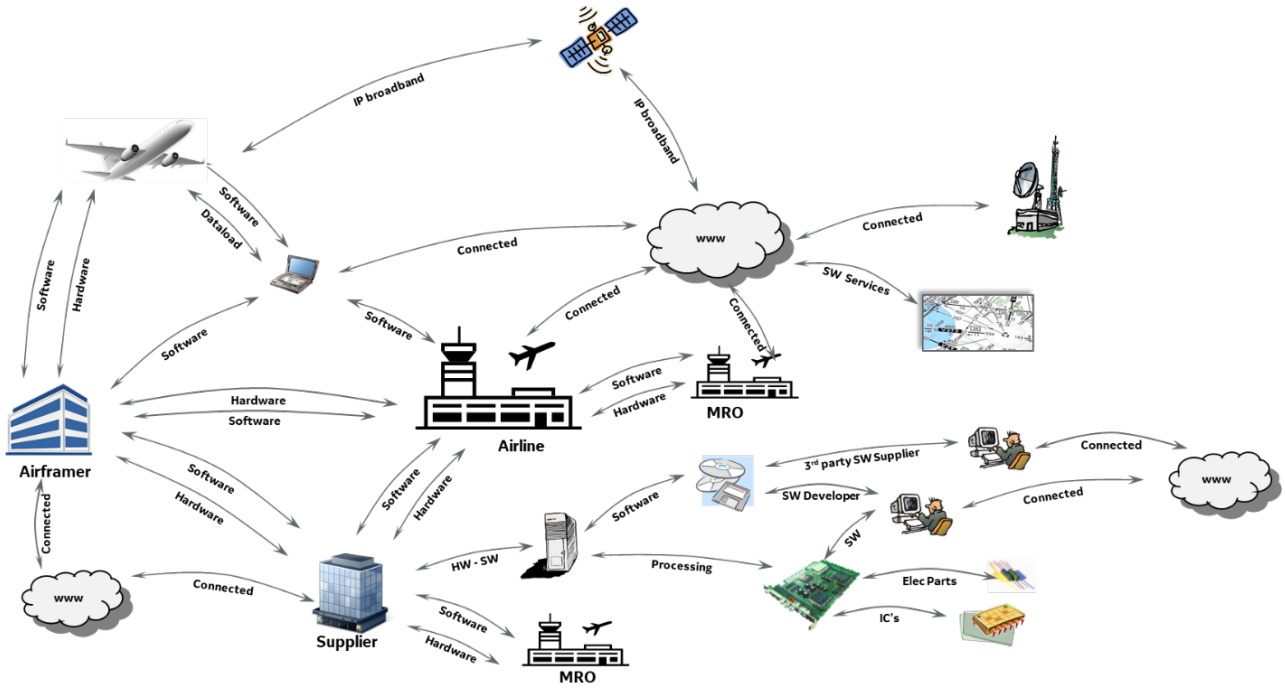

Figure 1: Securing the Aviation Ecosystem

2 Current State & Advancements

Since the issuance of the *AIA Civil Aviation Cybersecurity Software Distribution and Dataload Cyber Recommendations* report in February 2020, the aviation industry has taken significant strides in establishing standards and increasing availability of secure software distribution and loading tools.

ARINC 835 and ARINC 827 utilization within the aviation industry continues to increase. It provides options for software suppliers to implement digital signatures in multiple formats. Adherence to this standard helps ensure at least one of many acceptable digital signature formats are implemented and that the software part to be delivered (via secure digital distribution or through physical form such as CDs or Floppies) is packaged with an associated digital signature. This enables the digital signature to then be verified by an ARINC 645-1 compliant Portable Data Loader (PDL), Airborne Data Loader (ADL), or standalone devices such as a PC capable of verifying ARINC 835 and ARINC 827 based digital signatures and signed crates, respectively. It is important to note, ARINC 827 was designed as a point to point transfer mechanism, and not the end-to-end security that ARINC 835 provides. Thus, when utilizing an ARINC 827 solution for end-to-end security purposes, an ARINC 827 crate must retain all content and its cryptographic security file (crate.xml) throughout the distribution process so that a validity check can occur just before the software load process begins.

PDL manufacturers have also played a major role in continuing to advance PDL technology to strengthen the security mechanisms implemented in the data loader devices. These advancements not only provide protection against tampering of the PDL and ADL devices, but are also designed to protect software parts that are installed on-board and software at-rest.

ARINC 645-1 establishes security hardening requirements for PDLs and ADLs. It was updated throughout 2020 and issued in August 2021. In addition to making the loading devices more robust from a security standpoint, these devices are also aiming to a help make the verification of digital signatures on-board seamless to minimize and simplify additional steps operators and software loading personnel have to follow.

3 Secure Software Distribution & Loading – Phased Approach

To mitigate the risks posed on software distribution and loading, a phased approached is recommended to the industry. This approach aims to address the security risks while minimizing the burden on OEMs, suppliers, and operators to adhere to this proposed approach.

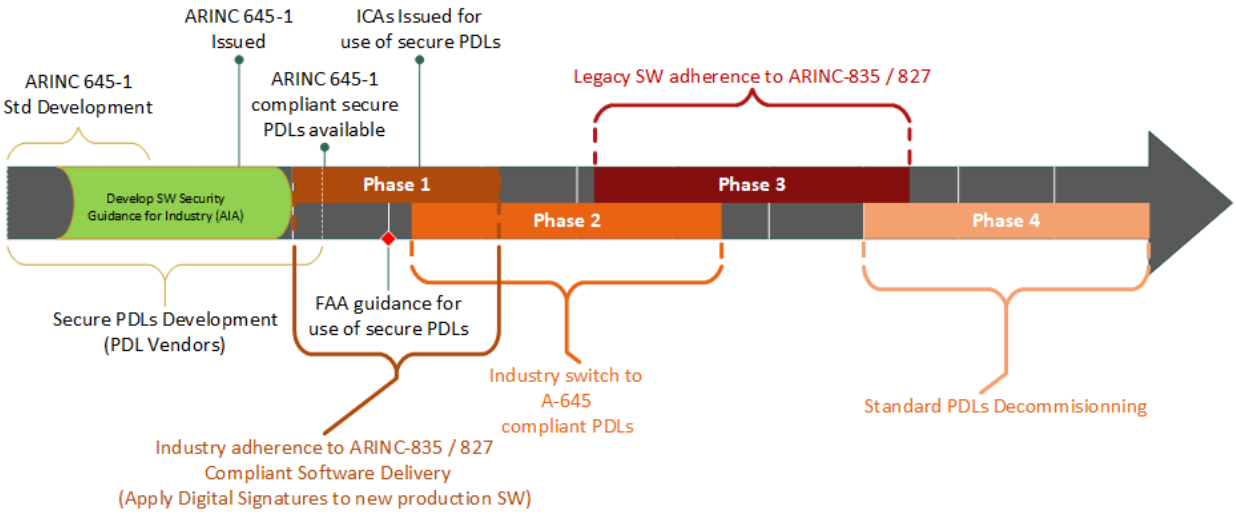

Figure 2. Phased Approach for Secure Software Distribution and Loading

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

3.1 Phase Overlap & Timeframe

Many aviation based companies have already begun delivering software with digital signatures and utilizing secure PDLs and ADLs to perform secure loading onto LRUs. However, in order to effectively mitigate the risks posed by tampered software, collective action is necessary. AIA understands the logistical complexities involved in availability and procurement of tools, financial burden, and level of effort required to fully transition between the proposed phases. Therefore, the phased approach provides a means for the industry to gradually transition through each phase in an effort to minimize disruptions, while allowing reasonable timeframe to adopt the security tools required to implement the digital signatures solution as well as procure secure PDLs, ADLs, and signature validation tools. The overlap between each phase is intended to allow use of current tools, and thus, prevent incompatibility disruptions, while companies develop and execute on transition plans.

It is also understood by AIA, due to the aforementioned challenges, that each industry OEM, supplier, and operator will have to transition through the phases on different timelines that suffice their own company's plan and per any dependencies involved with other industry businesses adopting the phased approach. It is imperative, however, that all parties involved take a proactive and diligent approach to reduce the risk exposure window as much as possible.

4 Phase 1 - ARINC 835 & 827 – Use of digital signatures for software distribution

Applying a digital signature provides software authenticity and integrity assurance. To ensure authentic, untampered software parts are loaded onto the aircraft LRU, application of a digital signature is strongly recommended. The signature should be applied by the software delivery source and validated upon receiving software into a company. Companies may want to add checks in various places along their internal distribution points to detect tampered software as early as possible, the signature should always be verified just prior to loading an aircraft LRU. This will provide assurance that the software, from the time it was in transit for delivery to being retrieved and potentially archived by the receiving party and being prepared for installation onto aircraft LRU(s) was untampered. Any intentional or unintentional changes to the software package content along any of those steps would invalidate the integrity checks performed during the digital signature validation. The certificate check also ensures that the source of the software can be trusted.

ARINC 835 provides two options for applying a digital signature, following established methodologies already in use within the aviation industry. Secure data loaders are also expected to be capable of verifying ARINC 835 and ARINC 827 signed software parts, thus, it is critical for software suppliers to adopt and implement one of three widely used signing methodologies used within the Aviation industry; ARINC 835 Airbus method, ARINC 835 Boeing method, or ARINC 827 (Method 1 - no LSP signing, but the crate's full contents are signed) to ensure all software parts to be distributed are digitally signed. In order to use an ARINC 827 signed crate, process steps must be implemented to allow validation of the signed crate by secure PDLs / ADLs. OEM and Commercial-Off-The-Shelf (COTS) tools are also available to help sign and validate software parts signed per ARINC 835 and/or crated per ARINC 827.

4.1 Applying digital signature(s)

When adding an ARINC 835 compatible digital signature to software parts or formatting the distribution software package per ARINC 827 signed crates, careful consideration should be given to any associated documentation that is necessary for field support personnel, such as instructions or procedures used for digital signature validation and software loading through a secure data loader. Field support personnel will

need instructions for what to do when a signature fails (i.e., Aircraft Maintenance Manuals, PDL procedures, etc.).

4.1.1 Digital Signatures Check Failures

Ground tools and ARINC 645-1 compliant data loaders may have to maintain updated Certificate Revocation Lists (CRLs). Users of these data loaders (e.g. operators) should define the acceptable maximum period of time allowed before the CRL is no longer valid. These CRLs are one of the elements used to validate the digital signature (depending on which ARINC 835 method is used) associated with the software part to be loaded. If the certificate associated with the digital signature is found to be revoked, ground tools, ARINC 645-1 compliant PDLs and ADLs should not allow the software part to be stored in the PDL/ADL and not allow software to be loaded onto an aircraft LRU.

Ground tools and ARINC 645-1 compliant data loaders may have to deal with expired certificates. If ARINC 835 timestamping is used, expiration may not have to be checked explicitly. Operators, OEMS, and suppliers should ensure that processes are in place to renew signatures where necessary, through manual or automated means. This could be incorporated as part of a Certificate Management life cycle program such as the one described in ATA Spec 42.

5 Phase 2 - Secure Software Loading

5.1 ARINC 645-1 Secure Software Loading

ARINC 645-1 compliant PDLs and ADLs are becoming more readily available to the aviation industry. These loaders are designed to the security requirements specified in ARINC 645-1 which help deter tampering with the loading device, contain security-based logs which can be helpful in investigations and cyber forensics efforts, and have capability to validate ARINC 835 based digital signatures of the software parts to be stored in the PDL/ADL and loaded onto the aircraft LRUs.

Transitioning from standard data loading solutions to ARINC 645-1 compliant secure data loaders provides additional safety measures in ensuring the correct and desired software part is loaded onto aircraft LRUs. Shop load tools and processes should also ensure that digitally signed parts are used for shop loading of LRUs. Generally, ARINC 645-1 loaders should also be used for shop loading.

AIA highly recommends aviation industry companies begin transitioning to use of ARINC 645-1 compliant data loaders. Some PDL vendors have now shown full compliance to ARINC 645-1, and as a result, secure PDLs devices are now available to the market for procurement.

While the overall transition is recommended to be done expeditiously, AIA understands there is a financial and logistical burden levied to industry operators, OEMs, and suppliers to replace fleets of standard data loaders with secure ones. Therefore, there are no exact compliance dates for the transition, rather the expectation is to transition to secure data loaders as soon as plausible for the PDL and ADL operators. To reduce the risk exposure window, it is imperative for each entity using PDLs or ADLs to, at a minimum, define and implement a transition plan to switch to secure loaders. This would help align with software suppliers' plans to deliver software with digital signatures which are expected to be validated by the recipient and would also help minimize disruptions to day-to-day operations when the switch to secure data loaders is completed.

5.1.1 Compliance recommendations

Advisory Circulars (ACs) 119-1 and 43-216 are currently being drafted to suggest the same software security mitigation outlined in this paper. Combined with guidance and mandates specified in ICAs from OEMs, there is a collective stance on securing software parts by encouraging the aviation industry to begin switching over

to use of digital signatures and secure data loaders. It is highly recommended all OEMs, suppliers, and operators take a proactive approach to ensure the transition from standard to secure data loaders is completed within a reasonable timeframe that is economically and logistically viable for the operators, OEMs, and aviation industry operators.

5.2 Ground Operations Process Security

Software being stored in production software storage vaults should be signed. Adding a digital signature prior to the software part(s) being stored protects the software at-rest. This also enables the software part to then be validated for authenticity and integrity upon retrieval from the storage vault, in advance of any distributions.

5.2.1 PDL Device Management Controls

Operators should implement strong physical and electronic access controls for PDLs to ensure that bad actors do not get access to loaders or the software parts stored on them. Operators must have processes to monitor and patch CVEs applicable to PDLs, and include periodic checks of PDL security based logs for detection of malicious activity, including, but not limited to tampering of the PDL device, unauthorized access attempts, unauthorized injection or extraction of third party applications to and from the PDL.

5.2.2 Media Management Controls

Operators should implement strong media handling and/or electronic protections for media that contains airplane software parts to prevent bad actors from accessing airplane software parts.

6 Phase 3 - Fielded Software Security

Software previously distributed without an accompanying digital signature, and if commissioned for loading on aircraft LRUs should be digitally signed prior to the next planned LRU load. The originator of the fielded software should also ensure that the software is digitally signed prior to any additional distributions.

7 Phase 4 - Decommissioning Standard PDLs & ADLs

To ensure secure software loading devices are the only ones used for aircraft LRUs, it is important for all industry groups to decommission standard PDLs and ADLs once they have completed replacements with secure data loaders. This includes shop loaders. Operators may wish to convert ADL airplanes to PDL connections if secure PDLs are more available or if this makes sense economically.

Each aviation entity with ownership of ADLs and PDLs should incorporate a plan for decommissioning the standard loading devices. As part of the decommissioning process these entities should also include a data purging step that removes all stored software parts, LRU downloaded data, and any other potential data of proprietary nature.

8 Adherence Timeframe

Since the initial release of this whitepaper, the aviation sector has made significant progress in raising awareness for the need to secure production software parts. Several industry level committees, including AIA, ARINC, and CSCAT have collaborated on promoting the need for the security measures discussed in the phased approach suggested in this paper. Overall, there is consensus within the industry to begin working through the recommended phases in a proactive manner.

Advancements in tool technologies, combined with their increased availability to market are making it more feasible for the industry companies to begin developing and executing their plan to comply with each phase.

In an effort to collectively and effectively mitigate the cyber safety risks associated with production software parts, AIA recommends the following timeframes for the industry to complete each phase.

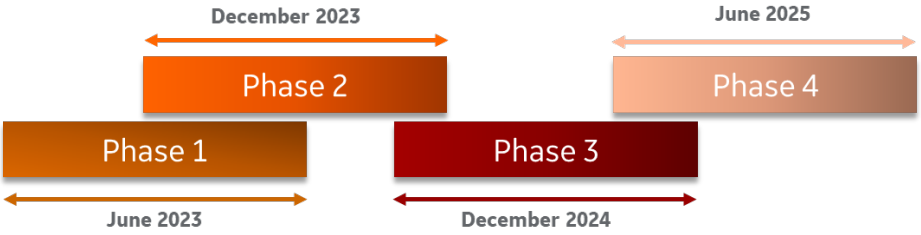

Figure 3. Phase completion recommendations

Regulators are reviewing software tamper risk based on certification submittals and incident responses. These activities may drive a more urgent timeline than desired by the industry.

Note that some of these phases may be able to occur in parallel depending on how ARINC 835 is implemented. The Boeing approach for example allows Boeing and operators to sign all software parts without phase 1 and phase 3 occurring first. Other implementations may require these to be in series. Either way, it is important to complete all phases to ensure software remains protected from its origin to the final step of being loaded onto an LRU or IMA.

9 Version History

Document Version	Description
1	Initial Release
2	Added recommendations for timeframe to adhere to the phased approach, including suggested timeline for industry companies to complete each phase.

10 Abbreviations

AC	Advisory Circular
ADL	Airborne Data Loader
AMC	Acceptable Means of Compliance
APIM	ARINC Proposal to Initiate/Modify an ARINC Standard
ATA	Air Transport Association
CA	Certificate Authority

COTS	Commercial Off the Shelf
CRL	Certificate Revocation List
CRI	Certification Review Item
CS	Certification Specifications
DAH	Design Approval Holder
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
ICA	Instructions for Continuing Airworthiness
ICAO	International Civil Aviation Organization
IMA	Integrated Modular Avionics
LRU	Line Replaceable Unit
MSD	Mass Storage Device
NIST	National Institute of Standards and Technology
NPA	Notice of Proposed Amendment
OEM	Original Equipment Manufacturer
OS	Operating System
PDL	Portable Data Loader
RMT	Rule Making Task
SDO	Standards Development Organization
UAS	Unmanned Aircraft Systems
USB	Universal Serial Bus

11 List of references

Reference	Title
AIA Civil Aviation Cybersecurity Subcommittee	Civil Aviation Cybersecurity Software Distribution and Dataload Cyber Recommendations Report, February 2020
ARINC 645-1	Common Terminology and Functions for Software Distribution and Loading
ARINC 827	Electronic Distribution of Software by Crate (EDS Crate)
ARINC 835	Guidance for Security of Loadable Software Parts Using Digital Signatures
ATA Spec 42	Aviation Industry Standards for Digital Information Security
CS-25	Certification Specifications for Large Aeroplanes
CS-29	Certification Specifications for Large Rotorcraft
CS-E	Certification Specifications for Engines
CS-P	Certification Specifications for Propellers

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