ARINC Project Initiation/Modification (APIM)

1.0 Name of Proposed Project APIM 19-011

Software Loader Security Guidance in Supplement 1 to ARINC Report 645: Common Terminology and Functions for Software Distribution and Loading

1.1 Name of Originator and/or Organization

Todd Gould, The Boeing Company

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

AEEC Software Distribution and Loading Subcommittee
Ted Patmore, Delta Air Lines (Chairman)

2.2 Support for the activity (as verified)

Airlines: American, Delta, Lufthansa

Airframe Manufacturers: Airbus, Boeing

Suppliers: Garmin, MBS, Safran, TechSat,

Note: Need confirmation: (Collins), (Honeywell), (Thales), (Teledyne), (Swiss Aviation Software)

Others: ICAO Aviation Trust Framework, AIA SW and Distribution Security Working Group**, RTCA, EUROCAE**

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: Delta,

Airframe Manufacturers: Boeing,

Suppliers: Garmin TechSat, Safran,

Others:

2.4 Recommended Coordination with other groups

(List other AEEC subcommittees or other groups.)

3.0 Project Scope (why and when standard is needed)

This project will have a high priority given that cyber security regulations and standards are being considered from work within ICAO, IATA, RTCA & EUROCAE, ARAC and ASISP. In this scope of work, these organizations are look to ARINC to define security process guidance to be implemented within aircraft software loading devices. This includes all types of civil aircraft types that use software loading devices, some of which are often referenced as dataloaders within the aerospace industry.

Civil aircraft cyber security is currently on the forefront of concerns within airline organizations and aircraft manufacturers. Work within standards organizations, as those previously indicated above, is in progress at an international scope. All aspects of cyber security threats, active measures, and security management are being considered and defined.

Data distribution and loading security, the process of securing software from the software provider to the aircraft flight systems, is the essential key vulnerability in the safety and security of all aircraft the use flight control software.

AIA software and distribution security working group has recommended that ARINC develop a security standard for all dataloaders, loader devices, portable dataloaders, STC airborne dataloaders, and shop loading devices.

3.1 Description

A variety of software loaders and load tools (PDLs and **STC** ADLs) are used to directly load aircraft systems onboard aircraft and load aircraft LRUs in supplier, OEM, and operator shops. The software load tools generally conform to ARINC 615, ARINC 665, and ARINC 615A standards. In general, most of these loaders do not implement ARINC 835 software security specification. Also, there is no common guidance on how the loaders operating system and media ports should be hardened against cyber threats. There is no common security process guidance for how the loaders should be managed or how the process of getting software to the loaders should be managed to be resilient against Cyber threats.

This standard would address the following to ensure a complete security solution is established for software loaders to be considered compliant:

1. Require use of adequate digital authentication mechanism to ensure aircraft software is not tampered with prior to any SW loading. ARINC 835 provides one example of a detailed description of industry implemented processes which can be used as a reference. However, compliance with ARINC 835 will not be required.
2. **Create or reference loader** device hardening requirements.
3. Create or reference processes for ensuring loader devices are developed to guard against cyber threats.
4. Create or reference processes for ensuring loader devices are well managed against cyber threats through all phases of the life cycle. For example, ensuring that the loading devices implement robust security measures to prevent corruption from untrusted networks; that loader device software is up to date, that loader devices are physically secured.
5. Create process recommendations for media handling and software transfer to the **loader devices** to ensure cyber resiliency.
6. PDLs and STC ADLs are specific examples of loading devices.

3.2 Planned usage of the envisioned specification

Note: New airplane programs must be confirmed by manufacturer prior to completing this section.

New aircraft developments planned to use this specification yes ☐ no ☒

Airbus: (aircraft & date)

Boeing: (aircraft & date)

Other: (manufacturer, aircraft & date)

Modification/retrofit requirement yes ☒ no ☐

Specify: This standard should be applied to all aircraft which use PDLs or **STC** ADLs.

Needed for airframe manufacturer or airline project yes ☐ no ☐

Specify: (aircraft & date)

Mandate/regulatory requirement yes ☒ no ☒

Program and date: It is expected that this standard would be used for operators to comply with AC 43-216. It is expected that regulators may require use of this standard in future rulings.

Is the activity defining/changing an infrastructure standard? yes ☐ no ☒

Specify (e.g., ARINC 429)

When is the ARINC standard required? __ASAP_____

What is driving this date? __AC 43-216 and AIA SW security use case

Are 18 months (min) available for standardization work? yes ☒ no ☐

If NO please specify solution: _____

Are Patent(s) involved? yes ☐ no ☒

If YES please describe, identify patent holder:

3.3 Issues to be worked

1. Device hardening requirements and potential impact to existing loaders
2. Regulatory involvement to ensure solution meets in work security rulings

4.0 Benefits

4.1 Basic benefits

Operational enhancements yes ☒ no ☐

For equipment standards:

(a) Is this a hardware characteristic? yes ☐ no ☒

(b) Is this a software characteristic? yes ☒ no ☐

(c) Interchangeable interface definition? yes ☐ no ☒

(d) Interchangeable function definition? yes ☐ no ☒

If not fully interchangeable, please explain: _____

Is this a software interface and protocol standard? yes ☐ no ☒

Specify:

Product offered by more than one supplier yes ☒ no ☐

Identify: All existing PDL and STC ADL suppliers are expected to be compatible with update security requirements

4.2 Specific project benefits (Describe overall project benefits.)

Provides the end of an end-to-end software tamper protection solution where the airplane OEMs do not provide a built-in secure loader.

4.2.1 Benefits for Airlines

Provides a more end-to-end solution that is less reliant on a variety of storage, network, and handling processes. Provides a good means to comply with AC 43-216.

4.2.2 Benefits for Airframe Manufacturers

Better assurance that all aircraft have better software tamper protection.

4.2.3 Benefits for Avionics Equipment Suppliers

Provides a security check right before loading into equipment.

5.0 Documents to be Produced and Date of Expected Result

Supplement 1 to ARINC Report 645 adding Software Loader Security Guidance

5.1 Meetings and Expected Document Completion

The following table identifies the number of meetings and proposed meeting days needed to produce the documents described above.

Activity	Mtgs	Mtg-Days (Total)	Expected Start Date	Expected Completion Date
Supp 1 to ARINC Report 645	*6*	*12*	*Oct 2019*	*May 2021*

6.0 Comments

The SDL Subcommittee has other APIMs in-work. Work on all projects are done in parallel.

The SDL has monthly web conferences to discuss and modify their assigned projects.

6.1 Expiration Date for the APIM

April 2022

Completed forms should be submitted to Paul Prisaznuk, AEEC Executive Secretary and Program Director (pjp@sae-itc.org).