

ARINC Project Initiation/Modification (APIM)

- 1.0 Name of Proposed Project** **APIM #: 23-xxx_____**
Securing Non-Safety Communications
- 1.1 Name of Originator and /or Organization**
KSAT Subcommittee
- 2.0 Subcommittee Assignment and Project Support**
- 2.1 Suggested AEEC Group and Chairman**
NIS Subcommittee
- 2.2 Support for the Activity (as verified)**
Airlines: United Airlines, American Airlines
Airframe Manufacturers:
Suppliers: Collins Aerospace
Others:
- 2.3 Commitment for Drafting and Meeting Participation (as verified)**
Airlines: United Airlines, American Airlines
Airframe Manufacturers:
Suppliers:
Others:
- 2.4 Recommended Coordination with other Groups**
KSAT
- 3.0 Project Scope (why and when standard is needed)**
- 3.1 Description**
Information that is communicated between devices represents a level of threat to the safety of the airplane and to the interests of the airline operator, the equipment suppliers, the service providers and the users, including passengers, cabin crew and flight crew.
System designers are tasked with assessing threats to the information that is communicated. The assessment is formally assessed for aircraft safety using RTCA DO-356A and other published methodologies. Adjacent to aircraft security are all the personal and business interests that are intertwined within the information. This APIM proposes to provide guidance for threat analysis applicable to information assets not related to aircraft safety. The process and guidance in RTCA DO-356A for threat assessment will be applied to non-safety information.

The following list provides a non-exhaustive list of examples of non-safety information, in the context of this APIM.

- Personally Identifiable Information (PII) and General Data Protection Regulation (GDPR) Compliance
- Financial Information and Payment Card Industry (PCI) Compliance
- Organization sensitive data
- Non-Safety function information not associated with the Data plane
 - Control plane
 - Maintenance plane

Each client application can apply security features themselves. Each client is a singular instance of varying levels of trust. The internetworking architecture and protocols are applied on top of client security features in a composite manner. Setting and aligning the expectations between client and the internetworks will allow a framework to build upon.

As time goes by, security objectives remain fixed while security features evolve. In some cases, security features are deprecated when shown to be inadequate due to evolving threat capabilities. As a result, this APIM describes a document that will need to be revised on a periodic basis to remain relevant and appropriate.

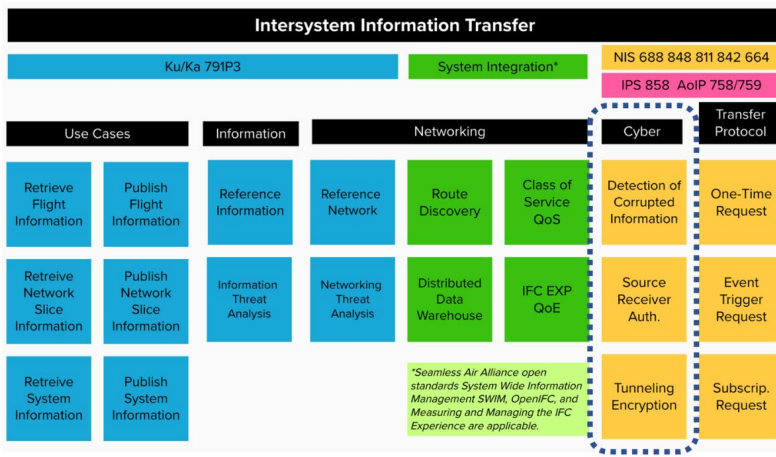
Many ARINC characteristics involve information transfer. The subcommittees responsible for each system have specific knowledge of their system interfaces and the information that is communicated. These subcommittees may list the interfaces and the security objectives for information communicated across each interface as part of their characteristic. Common security objectives are such as:

- Authenticating the source of information
- Assessing the integrity of information received
- Internet Access
- Using VLAN ID for information segregation
- Using IP subnetworks for information segregation
- Securing information from multiple domains across a common interface
- Information confidentiality
- Securing information across untrusted subnetworks
- Segregating information across Data, Control, and Maintenance Planes

System designers may align security objectives to relevant security features as provided using a common reference that may be applied to any system.

This APIM proposes to provide a mapping of recommended security features, or measures (e.g., protocols and architectures), for each security objective. This would include security features at the application layer, at the network layer and at the COTS (commercial-off-the-shelf) layer.

The boundaries between subcommittee and NIS are depicted in the figure below, for the example of ARINC 791 Part 3.



Commented [VM1]: Peter to update the image

In this example, the work of the Ku/Ka band subcommittee extends to documenting the information, the interfaces, and the threat analysis considering network architecture. This APIM proposes NIS to provide the document highlighted under Cyber. The Security Features listed are for example only.

3.2

Planned usage of the ARINC Standard

Note: New airplane programs must be confirmed by the aircraft 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: (aircraft & date)
- Needed for airframe manufacturer or airline project yes no
- Specify: (aircraft & date)
- Mandate/regulatory requirement yes no
- Program and date: (program & date)
- Is the activity defining/changing an infrastructure standard? yes no
- Specify (e.g., ARINC 429)
- When is the ARINC standard required?
- Not required but is needed to address best practices
- What is driving this date?
- 791P2 is contingent on NIS accepting the remaining portion of work described in this APIM.
- 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

- Roadmap from current state(s) to recommended state.
- Guidance for threat analysis not related to aircraft safety as it applies to information assets.
- Mapping of acceptable mitigations (protocol/architecture) for each threat level.

3.4

Security Scope

Is Cyber Security Impacted (if YES, check box(es) below) yes no

Aircraft Control Domain yes no

Airline Information Services Domain yes no

PAX Information and Entertainment Systems yes no

Other: _____ yes no

(Discuss the level of cyber security guidance needed, the specific topics to be covered, and whether these topics are covered elsewhere by reference, e.g., ICAO Documents, RTCA/EUROCAE Standards, existing ARINC Standards, or if they need to be defined by a new or revised ARINC Standard.)

4.0

Benefits

4.1

Basic Benefits

Operation 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: _____(company name)_____

4.2

Specific Project Benefits

Completing this work would provide guidance that would serve as a tool to harmonize best practices across all systems. This will help to avoid duplication of efforts (e.g., research, threat analysis, mitigations, etc.) within the various AEEC Subcommittee activities. Ultimately, this will provide a more resilient environment for non-safety.

This effort would prevent the unauthorized disclosure of information that could prove to be embarrassing or commercially threatening to passengers, the operating airline, and potentially any enterprise intertwined.

4.2.1 Benefits for Airlines

Completing this work would provide guidance that would serve as a tool to harmonize best practices across all systems.

This effort would prevent the unauthorized disclosure of information that could prove to be embarrassing or commercially threatening to passengers, the operating airline, and potentially any enterprise intertwined.

4.2.2 Benefits for Airframe Manufacturers

Completing this work would provide guidance that would serve as a tool to harmonize best practices across all systems.

4.2.3 Benefits for Avionics Equipment Suppliers/Service Providers/System Integrators

Completing this work would provide guidance that would serve as a tool to harmonize best practices across all systems.

5.0 Documents to be Produced and Date of Expected Result

Project Paper 8XX

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
8xx	5	15	06/2023	06/2026

The intent is to hold 5 meetings. Each meeting is 3 days each. This document will be worked at the same time as other documents and subjects within NIS. This effort will be supplemented by virtual meetings as needed.

6.0 Comments

Virtual meetings will be scheduled depending the level of effort needed for document development

6.1 Expiration Date for the APIM

October 2026

Completed forms should be submitted to (aeec@sae-itc.org)