ARINC Project Initiation/Modification (APIM)

1.0 Name of Proposed Project APIM 23-004

Securing Non-Safety SATCOM Communications

1.1 Name of Originator and /or Organization

Ku/Ka-band Satcom Subcommittee (KSAT)

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

Network Infrastructure and Security Subcommittee, Jeff Rae (United Airlines)

2.2 Support for the Activity (as verified)

Airlines: United Airlines, American Airlines, Southwest
Airframe Manufacturers: Boeing, Airbus
Suppliers: Collins Aerospace, Panasonic
Others:

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: United Airlines, American Airlines, Southwest
Airframe Manufacturers: Boeing
Suppliers:
Others:

2.4 Recommended Coordination with other Groups

KSAT, CSS

3.0 Project Scope (why and when standard is needed)

3.1 Description

Information that is communicated through Non-Safety SATCOM represents a level of threat 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 Non-Safety SATCOM internal and Non-Safety SATCOM client information assets not related to aircraft safety, without delving into every international privacy and security regulation. 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

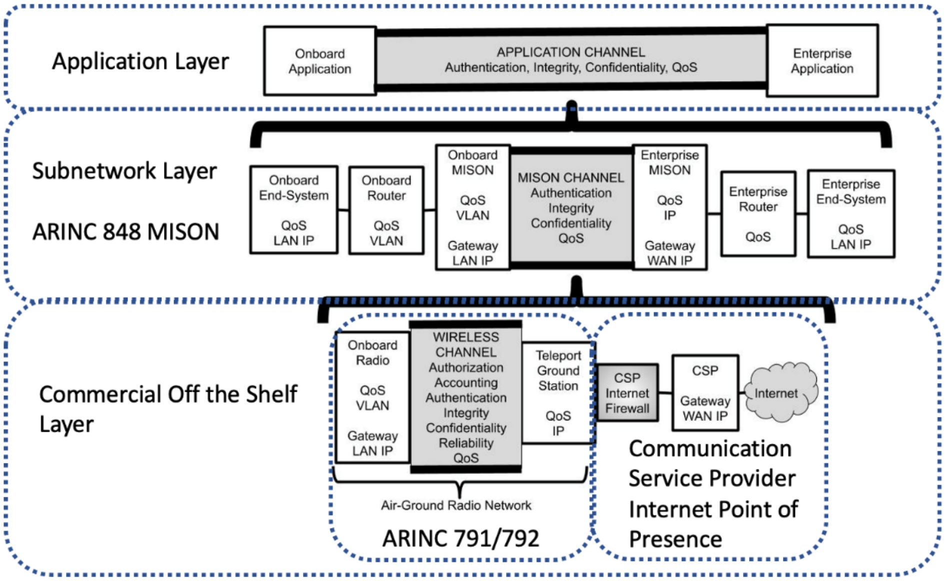
Each Non-Safety SATCOM client application can apply security features themselves. Each Non-Safety SATCOM client is a singular instance of varying levels of trust. The internetworking architecture and protocols are applied on top of client security features in a composite manner. Setting and aligning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

As time goes by, security objectives remain fixed while security controls evolve. In some cases, security controls 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.

Common KSAT security objectives are such as (preliminary list):

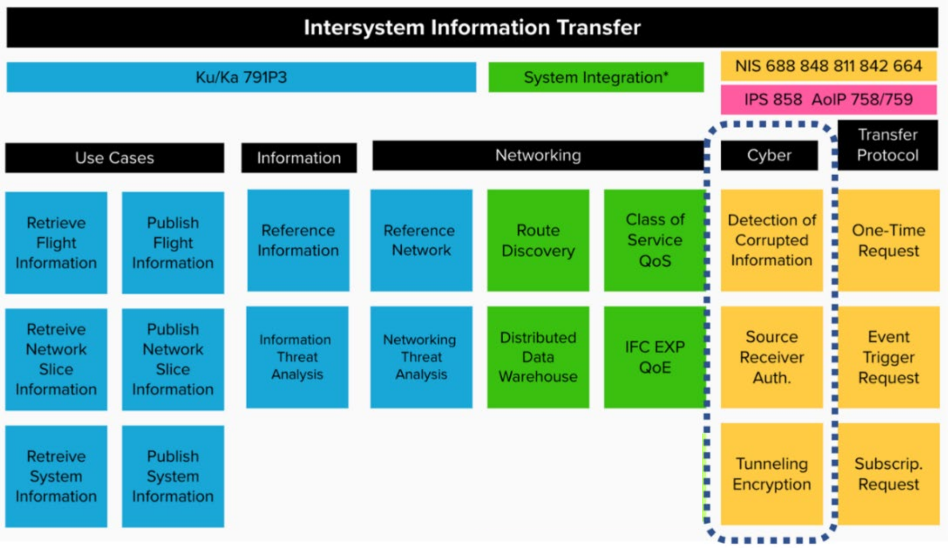
- Authenticating the source of information
- Assessing the integrity of information received
- Internet Access
- Using VLAN ID for information segregation
- Using IP subnetworks for information segregation
- Securing information from multiple domains across a common interface
- Information confidentiality
- Securing information across untrusted subnetworks
- Segregating information across Data, Control, and Maintenance Planes
- Preventing eavesdropping on the satellite data and control signals.
- Identifying key ownership and encryption responsibility, between the applications that use SATCOM, and the SATCOM subsystem itself.
- Best practices for key management

System designers may align security objectives to relevant security controls as provided using a common reference. Security controls may be applied within the SATCOM system, at the subnetwork layer, and at the application/client layer. Generic guidance will be provided since it must be given without a specific system configuration in mind, without knowing the operator’s risk tolerance, and without any knowing specific regional regulations that must be respected.



This APIM proposes to provide a mapping of recommended security controls, or measures (e.g., protocols and architectures), for each security objective. This would include security features at the application layer (onboard application to the connected enterprise application), at the subnetwork layer (interface between onboard application, SATCOM, and enterprise application), and at the COTS layer.

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



Intersystem Information Transfer

Ku/Ka 791P3

System Integration*

NIS 688 848 811 842 664

IPS 858 AoIP 758/759

Use Cases		Information	Networking			Cyber	Transfer Protocol
Retrieve Flight Information	Publish Flight Information	Reference Information	Reference Network	Route Discovery	Class of Service QoS	Detection of Corrupted Information	One-Time Request
Retreive Network Slice Information	Publish Network Slice Information	Information Threat Analysis	Networking Threat Analysis	Distributed Data Warehouse	IFC EXP QoE	Source Receiver Auth.	Event Trigger Request
Retreive System Information	Publish System Information					Tunneling Encryption	Subscrip. Request

In this example, the work of the Ku/Ka band SATCOM 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?

791P3 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. This will help to avoid duplication of efforts (e.g., research, threat analysis, mitigations, etc.) within KSAT and NIS 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.

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.

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.

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 on 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****)***