ARINC Project Initiation/Modification (APIM)

1.0 Name of Proposed Project APIM 19-004

New ARINC Project Paper xxx: Cabin Secure Media Independent Messaging

1.1 Name of Originator and/or Organization

Safran Aerospace

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

Cabin Systems Subcommittee (CSS)
Dale Freeman Delta Air Lines

2.2 Support for the activity (as verified)

Airlines: Delta, Etihad

Airframe Manufacturers: Boeing, Airbus

Suppliers: Safran Passenger Systems, Panasonic, Thales, Crane, Lufthansa Technik, Astronics, Zodiac Seats UK, KID Systeme, Recaro, BAE Systems, Diehl

Others:

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: Delta, Etihad

Airframe Manufacturers: Boeing, Airbus

Suppliers: Safran Passenger Systems, Panasonic, Thales, Crane, Lufthansa Technik, KID Systeme, Astronics, Recaro, BAE Systems, Diehl

Others:

2.4 Recommended Coordination with other groups

Network Infrastructure and Security (NIS) Subcommittee

EFB Subcommittee

SAI Subcommittee

3.0 Project Scope (why and when standard is needed)

3.1 Description

Refer to attached White Paper

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: (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

When is the ARINC standard required? _____(ASAP) _____

What is driving this date? Many existing integrations between different vendors of IFE & IFC

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

Define

- M2M messaging infrastructure services necessary to communicate with networked components based on selected IoT services and protocols (REST, CoAP or MQTT, DTLS, CBOR, etc.);
- Rules for URI mapping of device attributes and services for access by applications executing on other networked devices;
- Machine readable schema (e.g., JSON Hyper-schema) that will be used by suppliers and integrators to describe device interfaces, device interaction and path to source data;
- Common device attributes and services necessary to enable network integration, security, installation and management;
- Aircraft systems semantic ontology used to document device interfaces;
- Semantic ontological repository to allow open access for supplier contributions, configuration managed to support application developers and integrators;
- Subsystem and system verification testing approach based on declared component functionality and integrator defined components and information paths;

- Limited exposure of some component attributes and services and the manner in which they are made available for access by non-avionics data analytic maintenance applications.

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: (company name)

Panasonic Avionics Corporation
Thales InFlyt Experience
Safran Aerospace
Crane
Astronics
Recaro

4.2 Specific project benefits (Describe overall project benefits.)

4.2.1 Benefits for Airlines

Common messaging infrastructure across aircraft wired and wireless networks allows simplified system integration for aircraft functional expansion including new sensors, new applications and shared information across dissimilar networks to achieve improved operations and maintenance.

4.2.2 Benefits for Airframe Manufacturers

Similar to airline benefits

4.2.3 Benefits for Avionics Equipment Suppliers

Similar to airline benefits

5.0 Documents to be Produced and Date of Expected Result

ARINC 8xx new document, +18 months

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
Develop ARINC Project Paper xxx	4	4 (using 1 of 3 SC meeting days)	Oct 2019	May 2021

This effort is part of the larger Cabin Systems Subcommittee effort. The draft document will be discussed in periodic web conferences as needed.

6.0 Comments

N/A

6.1 Expiration Date for the APIM

October 2021

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

APIM 19-004

Cabin Secure Media Independent Messaging

Introduction

A typical aircraft hosts many networked systems from different suppliers. In most cases, these systems operate independently and, with limited exceptions, are unable to benefit from equipment commonality, integrated maintenance or centralized management.
New cabin system designs are beginning to integrate cabin functions in aid of overarching functions like data collection and off-load for predictive maintenance and the creation of expanded crew awareness such as display of cabin status including TTL safety checks on portable crew devices.
Expanded cabin functionality and cabin systems integration are expected to touch galleys, lavatories, passenger service units, entertainment services, window controls, lighting and many other systems.
Integration of systems from different suppliers is only possible if communications interfaces and protocols are standardized. Similarly, suppliers require common standards to affordably produce new devices that can communicate with and be easily integrated into a variety of cabin systems.
Wireless system intra-communications is rapidly becoming the preferred system architectural approach to achieve reduced weight, reduced cost and ease of system reconfiguration/expansion.
Onboard networks vary widely in their needs for power, throughput, distance, location, number of clients, etc. From a wireless communications perspective, one size does not necessarily fit all: different aircraft interconnect systems come with different technical problems and benefit from different network architectures and communications mediums, whether wired or wireless.
Ethernet, Bluetooth, WAIC, RFID, Wi-Fi, ZigBee –each technology has unique attributes that make it the most efficient and/or cost-effective solution for a specific onboard task.
A common inter-application communications infrastructure is required to enable onboard sensors, clients and applications to communicate and share information across a variety of task-optimized communications mediums.

Messaging

Application-to-application communications across dissimilar networks is common in the IP-world and has been further pushed forward in the commercial electronics industry through the development of communications standards for the Internet of Things (IoT), which includes a larger variety of different client platforms and network technologies.
Machine-to-Machine (M2M) communications between applications and IoT devices occur at the presentation and application layer of the OSI stack, thereby abstracting network-specific physical interfaces and protocols. Standards for M2M messaging on the IoT offer a well-defined framework that can be used for aircraft cross-system communications.
The IoT does not depend on fixed addresses or device-specific functions. Rather, IoT applications rely on a “discovery” process. When a new device is discovered on the network, an application can refer to a common Resource Repository to determine device capabilities and determine how to access the attributes and services of the new device. The discovery process allows new devices and new applications to be introduced to networks at will and it works

because IoT devices and applications use a common language to describe their capabilities and interfaces. When a new IoT device is attached to a home network its capabilities can be automatically discovered so its features and services can be incorporated by existing applications. While useful and clever in the home market, device discoverability is not necessarily a positive attribute in network environments with strict configuration management rules.

Aircraft networks employ fixed configurations, established by system integrators. Introducing IoT-type devices and communications into an aircraft environment will require certain standard adaptations to ensure adherence to aircraft certification and configuration management processes.

The overall utility of M2M communications for integration of new aircraft functionality will depend on standard definitions for device attributes and services that can be mapped by system integrators to manage the application interaction necessary to create new functionality.

The definition of a standardized M2M messaging interface for each avionics component enables the development and certification of new aircraft applications which can be introduced without impacting existing certifications.

Device Interface Definition Format

Traditional avionics suppliers provide an Interface Control Document (ICD) for each aircraft equipment that defines precisely how its attributes and services are accessed. An aircraft system integrator then utilizes equipment ICDs to define the system interconnections to distribute data from sources to destinations. This process works because RTCA/EUROCAE MOPS and ARINC documents exist which specify common interfaces between suppliers. It is also a fixed process that is slow and difficult to change. New sensor and wireless communications technologies are being developed at a rate that existing processes for equipment standardization can no longer support.

Interface definitions for IoT devices are written in a human-readable form. The most popular formats for interface definition are eXtended Markup Language (XML) or JavaScript Object Notation (JSON) schema. The interface definition for a given IoT device fully describes the accessible features of the device. An IoT device's interface schema is the functional equivalent of an aircraft equipment ICD. The structure of the device schema is usable by applications as an extension of the device address to access specific device attributes and services.

An IoT device's interface definition is described by the supplier in an importable schema. This same schema concept is used to describe the interface definitions of a subsystem. A system integrator defines new aircraft functions by linking function-specific applications to the imported attributes and services of member devices.

Core Device Features

System integrators depend on a common set of attributes and services from each network device to allow that each device to be incorporated and managed in a common manner. The following core services will enable system integrators to build network solutions from compliant avionics components:

- Authentication/authorization
- Remote (Wireless) Data load
- Configuration Management, including access controls
- Security/Cryptographic Key/Certificate Management

- Maintenance Services (BITE, etc.)
- Maintenance Logging and Reporting
- Security Logging and Reporting

Device Addressing

Aircraft network addressing must accommodate both wired and wireless devices in fixed or mobile operation. In any case, networks will no longer be dependent on fixed hardware adapter physical addresses (e.g. Ethernet). Instead, access to IoT devices will be based on web addressing using Uniform Resource Identifiers (URI). Access to individual device attributes and services will be accomplished by extending a device URI with the name of the attribute or service as defined in the semantic ontology. For example:

Each property or service in the device schema has a reference URI which consists of the device name with a concatenated name of the property or service.

e.g., “readingLight/on”

An integrator embedding a predefined device into passenger seat would import the device’s JSON schema and create an instance of the device schema. The URI to access a property or service of a device instance would be built by concatenating the name of the current container object (“seat”) with the partial URI from the embedded object to form a unique description.

e.g., “seat/readingLight/on”

Continuing with the seat example, one or more instantiations of the seat object can be embedded into a seat group. Each instance of seat is given a unique name. The URI to access any addressable element of an object in the seat group is built by concatenating the seat group name “seatGroup” with the name of an object instance e.g., “seat1” with the name of the device followed by the name of the property or service.

e.g., “seatGroup/seat1/readingLight/on”

This same process occurs as the cabin integrator embeds instances of seatGroup into a Row schema and instances of Row into a cabin schema.

e.g., “Row/MiddleSeatGroup/seat1/readingLight/on”

becomes

“LH748Cabin/Row33/MiddleSeatGroup/seat1/readingLight/on”

The only remaining step for the system integrator is to concatenate the link type and authority address with any URI address chain to derive a fully formed address to a parameter on the network.

e.g.,
“coap://192.168.1.1/LH748Cabin/Row33/MiddleSeatGroup/seat1/readingLight/on”

The above integration process can be highly automated and can be fully verified at every subsystem step to significantly simplify the total aircraft-level integration effort.
Each subsystem can limit how many of its internal attributes and services are accessible by only exposing some attributes and services in its schema that will be imported for integration on other systems.
The nested subsystems in the above example also illustrate how subsystem testing can be accomplished within the IoT metaphor. Every subsystem (e.g., seat) is independently testable since the subsystem schema fully defines the attributes and services available for communications with other systems.

Semantic Ontology

IoT applications are able to establish communications with new IoT devices on the network because they share a common descriptive language for defining device capabilities, attributes and methods and a common M2M messaging service for communicating between devices. A Semantic Ontology is the common dictionary for a collection of IoT devices.
Semantic ontologies tend to differ from one industry to another and are typically built from modular device ontologies such as the Semantic Sensor Network Ontology on the World Wide Web. Industry-specific semantic ontologies are hosted on W3.org so as to be universally accessible by device developers and system integrators. The medical and automotive industries have semantic ontologies on W3.org. No semantic ontology exists for the aviation industry on W3.org today.
A semantic ontology for the aviation industry must be built based on a common base object that defines all of the standard attributes and services which every other aviation device will inherit. Avionics suppliers define new device interfaces based on the terminology used in the semantic ontology. The semantic ontology will expand as new and unique device capabilities are incorporated into the ontology by equipment suppliers.

RTCA DO-356A Security Compliance

RTCA SC-236 Wireless Avionics Intra-Communications (WAIC) is currently defining equipment and network requirements for wireless avionics communications devices operating in the 4.2-4.4 GHz band. SC-236 performed an analysis based on DO-356A/ED-203A security guidelines which identified vulnerabilities associated with authentication, data load and configuration of wireless equipment on aircraft. SMIM requirements will address these vulnerabilities to ensure networks that use SMIM are capable of DO-356A/ED-203A compliance when using either wired or wireless media types.

Key Tasks

The ARINC Specification must specify:

- M2M messaging infrastructure services necessary to communicate with networked components based on selected IoT services and protocols (REST, CoAP or MQTT, DTLS, CBOR, etc.);
- Rules for URI mapping of device attributes and services for access by applications executing on other networked devices;

- Machine readable schema (e.g., JSON Hyper-schema) that will be used by suppliers and integrators to describe device interfaces, device interaction and path to source data;
- Common device attributes and services necessary to enable network integration, security, installation and management;
- Aircraft systems semantic ontology used to document device interfaces;
- Semantic ontological repository to allow open access for supplier contributions, configuration managed to support application developers and integrators;
- Subsystem and system verification testing approach based on declared component functionality and integrator defined components and information paths;
- Limited exposure of some component attributes and services and the manner in which they are made available for access by non-avionics data analytic maintenance applications.

While the above list of tasks may initially appear daunting for the development of a new ARINC Specification, this activity can pull extensively from existing IoT standards and emulate semantic ontology models developed for the medical and automotive industries to reduce the total project effort.

.