ARINC Project Initiation/Modification (APIM)

Note: This draft APIM was approved by the AEEC Executive Committee on November 1, 2013 with the proviso that proponents update it to reflect the concerns stated at the AEEC Mid-Term Session held in Zagreb, Croatia by Airbus. See Attachment 2 to reference letter 13-160/AXX-179.

A revised draft is expected in early 2014.

1.0 Name of Proposed Project APIM 13-005

Security Data Logging

1.1 Name of Originator and/or Organization

Steve Arentz, United Airlines / Ted Patmore, Delta Air Lines

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

Network Infrastructure and Security (NIS) Subcommittee

Steve Arentz, United Airlines and Jean-Paul Moreaux, Airbus

2.2 Support for the activity (as verified)

Airlines: United Airlines, Delta Air Lines, American Airlines, Lufthansa, FedEx [TBD], Southwest, USAF, TAP Portugal, UPS

Airframe Manufacturers:

Suppliers: GE Aviation, Teledyne, Rockwell Collins

Others: VOLPE

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: United Airlines, Delta Air Lines

Airframe Manufacturers:

Suppliers: GE Aviation, Teledyne, Rockwell Collins

Others: VOLPE

2.4 Recommended Coordination with other groups

RTCA SC 216 subgroup 4 and EUROCAE WG-72

3.0 Project Scope (why and when standard is needed)

3.1 Description

Newer aircraft have systems which generate logs that are stored on board, and are downloadable to portable media or ground equipment mass storage. These logs are currently structured into various formats that are specific to each aircraft type and system. Therefore, there is no common standard for structure and content. Additionally, some of the data currently collected within these log files may not be within the scope of security related information that is required to perform security threat analysis on ground tools.

Currently, there are no specifics as to what events are logged, how frequently they are sampled, or the format in which this data is stored.

Part of the RTCA/EUROCAE effort is the development of a document titled “Information Security Guidance for Continuing Airworthiness”. One of the guidance elements defined within this document is for operators to download and analyze these log files for possible security threats periodically.

For these reasons, there is a need to define the types of information required for security log file analysis.

Objective of this APIM:

The objective of this project is to establish a common set of security related data elements and format(s) that are produced by the avionics systems and can be used by Airline IT and/or avionic supplier ground tools in the analysis of aircraft security log file data.

- Facilitate a common set of log file data from various aircraft types that can be filtered and/or translated to a common data format(s) which can be input into IT ground tools for analysis.
- Avoid multiple data formats, and the need to develop multiple ground tools to process them.
- Define standard data element classifications (e.g. threat levels) associated with possible security threats.
- Provide the ability to have a consistent means of performing security analysis of log file data.
- Provide a standard for security logging and file generation for new implementations.
- Establish an industry standard set of data elements for aircraft security logs will provide a degree of consistency.
- Standardize security data to facilitate common security analysis methods, help establish security analysis policies and measure their effectiveness across the commercial aircraft industry.

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: general applicability to future work
Boeing: general applicability to future work
Other: general applicability to future work

Modification/retrofit requirement yes ☒ no ☐

Specify: general applicability to future work

Needed for airframe manufacturer or airline project yes ☒ no ☐

Specify: general applicability to future work

Mandate/regulatory requirement yes ☐ no ☒

Program and date: security logging requirements

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

Specify (e.g., ARINC 429)

When is the ARINC standard required? April 2016

What is driving this date? Need for global solution for logging

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

If NO please specify solution: __________________

Are Patent(s) involved? yes ☐

If YES please describe, identify patent holder: __________________

3.3 Issues to be Worked

- Collect current existing log data from various sources to establish a baseline for standard security related data collection types.
- Define a standard set of information types (data elements) that should be stored, monitored, and analyzed for the presence of security issues.
- Define functions/processes for conversion of aircraft data logs into a standard data set for ground use.
- Each information type that is defined should have an explanation of why it is included in the data set, and how it can be used to expose potential security threats.
- Pool together input from all OEM subject matter experts on log files that are currently in use to discover and establish security data that is common to all log files in used today.
- Establish a framework for continuous improvement of security log analysis as the industry gains experience with aircraft information security analysis and mitigation.
- Overall monitoring, analyzing, and responding to security events/audit logs need to be addressed in this effort.

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)

4.2 Specific Project Benefits (Describe overall project benefits.)

Regulatory compliance and safety.

4.2.1 Benefits for Airlines

RTCA SC 216/EUROCAE WG 72 is producing a document that will provide guidance to airlines that are required by regulators to manage security log files. To do this, airlines need to be able to:

- Ensure that necessary technical information about the aircraft security log files is available (e.g. data dictionary)
- Maintenance instructions and tools for download
- Define triggers or frequencies for download aircraft security log files
- Define procedures for transferring, storing and safeguarding of aircraft security log files off aircraft (ensuring confidentiality, integrity, authenticity and availability)
- Define retention times for aircraft security log files
- Ensure guidance for review and analysis of security log files is available (including event signatures, associated root causes and recommendations for reaction)

Standardization of log data content types will be required for airlines to perform some of the above processes effectively and efficiently, especially the review and analysis parts. Airlines will realize a significant cost savings by having a common log data format by avoiding the necessity of having multiple job roles for the management of non-standard log data.

- It is expected that the number of airlines performing the analysis will continue to grow. This would include all flights and aircraft for the particular airline. Establishing this process will reduce considerable effort to integrate the information into an airline's existing IT data collection and analysis ground-based tools. In addition, it will minimize any new burden on the airlines as a result of collecting and storing large amounts of aircraft log data.
- Using one common log data set will also facilitate a standard methodology for analyzing the security log data, which will minimize the airline's reoccurring cost of analyzing and processing log data.
- It will facilitate airlines being able to import logs from all aircraft into their ground analysis tools thus avoiding costs of multiple tool types and personnel for each.
- A standard that defines the log information would reduce the cost of the integration activities, and allow for a standard solution that can be reused rather than reinvented each time.

4.2.2 Benefits for Airframe Manufacturers

The FAA has required that 787 retain logs for at least 90 days. Regulatory authorities are increasingly interested in security logs generated by onboard systems. This will be required to enable measuring of security effectiveness, establishment of security policies related to log file management and analysis.

It is anticipated there will be changes/costs associated with development of this effort, however it is also anticipated that ongoing support costs will be reduced.

This effort foresees reduced repetitive cost through standardization which is passed down to avionics equipment suppliers and on into their retrofit products. Ultimately this would benefit airframe manufacturers.

4.2.3 Benefits for Avionics Equipment Suppliers

Onboard avionics equipment generates logs in different ways and provides various methods in transferring the data for off-board analysis. Typically, these files then need to be imported into existing ground analytic tools. Many of the benefits outlined for the airlines would apply to the avionics equipment suppliers as well.

The coming aircraft information security compliance requirements create the need for all industry stakeholders to be as efficient as possible in their processes and reduce repetitive cost through standardization.

5.0 Documents to be Produced and Date of Expected Result

ARINC Project Paper 8xx: Standardized Security Logging Guidelines

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
NIS SC	*6 meetings* *(3 days each)*	*18*	*Apr 2014*	*Oct 2016*

Please note the number of meetings, the number of meeting days, and the frequency of web conferences to be supported by the IA Staff.

6.0 Comments

Physical meetings would be augmented as needed with teleconferences.

6.1 Expiration Date for the APIM

April 2017

For IA staff use only

Date Received: IA staff: ____________

Potential impact: ______

*(**A**. Safety **B**. Regulatory **C**. New aircraft/system **D**. Other)*

Resolution: _______

Authorized, Deferred, Withdrawn, More Detail Needed, Rejected)

Assigned to SC/WG:________________

Completed forms should be submitted to the AEEC Executive Secretary.