Terms of Reference

Initial

Special Committee 216 / EUROCAE Working Group 72

Aeronautical Systems Security

1. REQUESTER AND SPECIAL COMMITTEE VOLUNTEER LEADERSHIP:

<table>
<thead>
<tr>
<th>Person</th>
<th>Requester</th>
<th>Co-chairman</th>
<th>Co-chairman</th>
<th>Designated Federal Official</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Munir Orgun</td>
<td>Chuck Royalty</td>
<td>Dan Johnson</td>
<td>Raymond Decerchio</td>
</tr>
<tr>
<td></td>
<td>Boeing Commercial Airplanes</td>
<td>Boeing Commercial Airplanes</td>
<td>Honeywell Aerospace Electronic Systems</td>
<td>Technical Programs and Continued Airworthiness Branch, AIR-120</td>
</tr>
<tr>
<td>Fax</td>
<td>425-717-5052</td>
<td>202-385-4651</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:Munir.orgun@boeing.com">Munir.orgun@boeing.com</a></td>
<td><a href="mailto:chuck.royalty@boeing.com">chuck.royalty@boeing.com</a></td>
<td><a href="mailto:daniel.p.johnson@honeywell.com">daniel.p.johnson@honeywell.com</a></td>
<td>Raymond <a href="mailto:W.Decerchio@faa.gov">W.Decerchio@faa.gov</a></td>
</tr>
</tbody>
</table>

2. DELIVERABLES:

The following deliverables and timetable assume that RTCA Inc. and EUROCAE approve the sponsorship of a joint special committee/working group, and develop a Work Programme that supports these deliverables and dates.

Product Documents

   The MASPS document should specify security information that should be useful to designers, manufacturers, installers and service providers for Aeronautical Electronic and Networked Systems.

   The processes and methods document should propose guidance for systems affected by security considerations to be developed and assessed, such that compliance with FAR 25.1309 can be demonstrated. This document may draw on ARP 4754, DO-178B, DO-254, and other material in addition to the security standards below to develop an acceptable security assessment and assurance process that can be used to show compliance with airborne systems safety regulations.

3. TERMINATION OF COMMITTEE ACTIVITIES
   Special Committee 2XX will terminate its activities when the Program Management Committee (PMC) and EUROCAE Council approve the committee’s final documents listed in section 2 of this Terms of Reference. Any change/extension of the committee’s work program requires prior PMC / EUROCAE Council approval.
4. AIRSPACE INFRASTRUCTURE LINKAGE
The International and National Airspace Systems (NAS) characterize the inter-relationships of aircraft operating in the airspace using the existing infrastructure and related Air Traffic Management (ATM) and Communications, Navigation and Surveillance (CNS) equipment, both ground-based and airborne. SC-2XX / WG 72 recommendations and guidance material will help ensure safe, secure and efficient operations amid the growing use of highly integrated electronic systems and network technologies used on-board aircraft and for CNS/ATM systems and air carrier operations and maintenance.

5. REQUIREMENTS ASSESSMENT:
Existing aircraft system safety guidance does not specifically address airborne network and data security issues, which results in non-standardized and potentially inequitable agreements between the various applicants and the various regulatory agencies on an acceptable process and means of compliance for ensuring safe, secure and efficient aircraft network design and operations. Also, existing information technology (ground-based systems) network and data security assurance processes are not easily adapted to the aviation system environment and do not address aspects of ATM/CNS ground-based and aircraft systems.

This Special Committee is needed to bring together aircraft manufacturers and systems designers, CNS/ATM systems designers and operators, airlines maintenance and operations personnel and government (primarily DHS/TSA, FAA, DoD) to form a consensus and document guidance for a network security assurance process and acceptable means of compliance for safe, secure and efficient airspace operations.

6. TERMS OF REFERENCE:
The Special Committee must examine the guidance provided by the following documents including but not limited to Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) documents to determine if these documents are sufficient to provide security assurance guidance for aircraft information systems.

FIPS 140-2, “Security Requirements for Cryptographic Modules”
FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
NIST SP 800-64, “Security Considerations in the Information System Development Life Cycle”
NIST SP 800-23, “Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products”
NIST SP 800-53, “Recommended Security Controls for Federal Information Systems”

These documents must be used as a baseline for the Special Committee work to ensure aircraft aeronautical systems and network security compatibility with the United States National Air Space (NAS) infrastructure. If the FIPS and NIST documents do not provide sufficient security assurance guidance for aircraft aeronautical systems, then additional proposed guidance should be documented in the products of this Special Committee. The committee must not propose any aircraft standards that will conflict with the existing standards from FIPS, NIST and ICAO on information security. The internationally accepted standard ICAO 9705, Manual of Technical Provisions for the Aeronautical Telecommunication Network
(ATN) – Third Edition (or latest version) for Data Communications Security, published by ICAO must be used as the basis for all information security requirements for Controller to Pilot Data Link Communications (CPDLC).

The special committee should, along with EUROCAE WG-72, develop a work program, with schedule and milestones, to accomplish the following terms of reference:

A. Develop guidance material that, at a minimum:
   b. Identifies network and data security issues that may impact aircraft safety and those where the impact is more business or privacy related, yet still important.
   c. Establishes assurance levels for security that relate to existing safety assurance (e.g., AC/AMJ 25.1309) criteria and levels and provides objectives for evaluating network security implementations
   d. Contains acceptable methods of demonstrating system safety when security issues impact existing airspace and aircraft safety methods of compliance.
   e. Addresses recording and responding to security “events” and guidelines for operations, continued operational safety and maintenance of security features.
   f. Addresses the requirements and guidance for post-response recovery, including identification of affected systems, restoration of system configurations, notification requirements, and other related activities.

B. Develop guidelines that, at a minimum:
   a. Will help aircraft manufacturers, system developers, operators, CNS/ATM providers and those responsible for implementation and operation of the airspace and aeronautical systems ensure the systems comply with the guidance material and maintain required levels of safety where security vulnerabilities have been identified.
   b. Identify attributes and characteristics of architectures and designs that constitute good practice, or which should be considered as basic to aeronautical security implementations.

C. Scope.

The general scope of this document is on non-airborne systems and human access (deliberate, casual, or accidental) to aircraft networked electronic systems and the impact of that accesses on airworthiness and the safety of flight.

The material developed by this SC will encompass the following:
   a. Security threats can be identified as those that impact aircraft safety and those that have business or privacy implications, but no impact on safety of flight. This SC will only develop guidance material that addresses the impact of non-airborne systems and human access to aeronautical systems that may impact airworthiness and safety of flight.
   b. Airborne systems and equipment:
      i. All aircraft systems electronic equipment, such as those used for flight management, navigation, communications, control of the airplane, information, maintenance, passenger services and entertainment.
      ii. Electronic networks used for on-board data exchange and for information exchange with systems external to the airplane.
   c. Assumptions about and considerations for the impact of security on airborne systems and equipment from aircraft external systems, including, as necessary, means for the evaluation and assessment of such systems in terms useful to airborne security processes. The following systems will be considered, but only the portions that have an effect on aircraft safety:
      i. ATC/ATS/CNS systems
      ii. Airline-owned systems
iii. Airport-owned systems
iv. Private network service providers

The SC will not address:

a. Other aspects of safety already addressed in existing guidance material, such as AC/AMJ 25.1309, ARP 4754, DO-178B, DO-278, and DO-254, except to the extent where there is a reliance on those other means of compliance.
b. Physical security or physical attacks on the aircraft (or ground element)
c. Airport, Airline or Air Traffic Service Provider facility security (e.g., access to airplanes, ground control facilities, data centers, etc.)
d. Those portions of airborne systems and external communications systems that do not have an effect on aircraft safety.

D. This SC will serve as a resource and coordinator for security-related issues and solutions with all RTCA Special Committees. This advisory and coordination role is not intended to include the imposition of specific security implementation designs or technologies into the standards being developed by the other SCs.

E. Coordinate with other groups and organizations (e.g., ARINC Network Infrastructure and Security Subcommittee, ATA Digital Security Working Group, SAE-XX, ICAO, etc.) including recommendations for changes/additions to standards and materials produced by those groups and organizations.

F. Actively pursue formation of a joint activity with EUROCAE WG 72.

G. Develop a work program and “packaging” proposal for review and approval by the PMC. Report to the PMC the direction being taken by the committee within 6 months after the first SC meeting.

7. OTHER CONSIDERATIONS:

During preparation of its deliverables, the SC should:

1. Emphasize that security should be considered early in the aircraft and network design and from an aircraft systems perspective.
2. Recognize the international implications of Aeronautical Network System Security and that aircraft operate globally.
3. Consider emerging technology and systems.
5. Develop, to the extent possible, an approach (or approaches) that accommodate changes in technology and that recognizes that aeronautical network system security is an on-going process (continued operational safety) and more involved than a single point-in-time analysis (operations, maintenance of security features). The material should focus on security objectives rather than specific solutions that may become obsolete in the future.
6. Consider the unique role that cryptographic technology plays in typical network security architectures. Determine what design and operational compliance methods are appropriate and adequate for the application of this technology to safety-related functions.
7. Recognize that today, the airworthiness of Aeronautical Networked Systems is largely maintained by Airline processes and procedures approved by regulatory agencies, and that Aeronautical System Security will likely be maintained in a similar manner by the same people.

EUROCAE

RTCA SC-2XX is anticipated to work jointly with EUROCAE WG-72.