EUR: 014-21 / WG96-69
RTCA Paper No: 013-21/SC236-044 November 12, 2021

Minutes of Meeting

EUROCAE WG-96 RTCA SC-236 20th Joint Meeting

Standards for Wireless Avionics Intra-Communication System (WAIC) within 4200-4400 MHz

Date	***Thursday November 12, 2020 15 - 18pm CET (9am – 12pm EDT)***
Hosted by	***RTCA and EUROCAE***
Place	***Virtual Meeting***
Contact Person	EUROCAE WG-96: Anna Guégan anna.Guégan@eurocae.net Phone: + 33 1 49 46 19 67 And RTCA SC-236: Rebecca Morrison rmorrison@rtca.org +1 202-330-0654

AGENDA

1. Welcome/Administrative Duties/EUROCAE and RTCA Policy Statements
2. IPR / Membership Call-Out and Introductions
3. Review and Approval of the Minutes from the 19th Joint Meeting
4. Review and Approve TOR changes for SC-236 and for WG-96
5. Define the path forward
6. New Business
7. Review Plan for Next Meeting
8. Review Action Items

EUROCAE WG-96 RTCA SC-236 20th Joint Meeting
Minutes of Meeting

Steve Rines (AVSI) started the meeting at 9:05 AM EDT.

Agenda Item 1: Welcome/Administrative Duties/EUROCAE and RTCA Policy Statements

Steve welcomed the committee members.

Rebecca Morrison read the relevant RTCA anti-trust policy and proprietary information and membership policy statements and Anna Guégan read the relevant EUROCAE policy statements from slides shared with the group. EUROCAE and RTCA will take action to ensure that committees stay compliant with these policies. It was noted that RTCA and EUROCAE honor each other's policies in the work of joint committee such as this in order to produce harmonized standards.

Agenda Item 2: IPR / Membership Call-Out and Introductions

Committee members introduced themselves.

Agenda Item 3: Review and Approval of the Minutes from the 19th Joint Meeting

The minutes from the 19th Joint Meeting were reviewed and approved.

Agenda Item 4: Review and Approve ToR changes for SC-236 and for WG-96

Recognizing the impasse in reaching consensus on allowable emitted power levels, Steve proposed changes to the ToR and ultimate TSO to separate the systems and security issues from the RF considerations so that the Committee could continue making progress on the MOPS.

This would lead to a MOPS for secure avionics communications across shared access networks (including wireless), using wireless networks as a worst case for security and availability to define a generic architecture capable of executing safety-related functions. The MOPS would seek to define an architectural model that isolates subnets while enabling functional information to be exchanged across networks of varying integrity.

The primary topics to be covered in a new MOPS would include

- Zero Trust Architecture Required Features
- Common Hardware Requirements
- Common Software Requirements
- Installation Requirements
- Certification Guidance and Processes

Steve described additional details of each of these topics.

Zero Trust Architecture Required Features

The MOPS would need to define requirements in terms of architectural features necessary to achieve autonomous, interconnected Zero Trust networks. These include a fixed network configuration in aid of restoration to known aircraft configuration, full function device (FFD) and reduced function device (RFD) feature definition, requirements on FFDs that act as gateways between subnets and networks, interoperability requirements (in concert with guidance being developed by ARINC) in aid of maintaining subnet autonomy while enabling remote network

management, configuration reporting, fault/status reporting, device modification, and multi-path network solutions for improved availability.

Common Hardware Requirements

The MOPS will need to define common network hardware component requirements including the FFD and RFD minimum hardware complement, hardware-based authentication/encryption, and equipment compliance certification testing along the lines of the NIST 800-193 test suite.

Common Software Requirements

The MOPS will also need to define common software requirements such as secure data load (including data loader requirements), data load packaging (including network associations and certificates), self-generated certificates for authentication and information exchange, background integrity checking to limit exposure to damage or attack, secure messaging for information exchange between network entities, and secure messaging minimum requirements.

Dave Redman asked if it would be necessary to duplicate or incorporate by reference requirements from the new ARINC standard and if that would be an issue for a TSO? Steve indicated that the MOPS will likely point to the ARINC standard as an acceptable means of certification, but not repeat requirements in the MOPS.

Installation Requirements

The MOPS will also consider minimum installation requirements necessary to meet the defined performance requirements. This includes hardware integration and verification in advance of installation (i.e., a fixed network configuration defined by the system integrator), unique equipment ID assignment, implementation of manufacturer equipment ID's versus unique device identifiers (UID) for use in data load, and associating UID with equipment installation location as part of data load sequence.

Steve described that the intent is to extend concepts from system modeling, where functions are implemented in an architecture with configurable end item components and installed equipment is assigned a binding based on the architecture to create a specific instantiation.

Certification Guidance and Processes

Finally, to provide a basis for the associated TSO, minimum system and process requirements need to be defined to allow certification by *function*. This will include references to existing guidance such as system safety assessment (SSA) and system security assessment by function, compliance with published security guidance from RTCA/EUROCAE SC-216/WG72, system features necessary to allow information to flow across networks of lesser integrity, separating system security from functional availability, functional verification testing against installed system performance, making SSA and system performance information available to third party integrators to allow integration of new functionality, and data handling associated with data load in compliance with ATA Part 42.

Kevin Hallworth noted that not all the interfaces may be available, which would imply that you might need to have a simulator on the ground for an installation assignment to be verified as correct. Steve commented that that is not really different than other complex avionics.

Steve explained that this is a new approach that can be described as "certification by function." Current methods rely on certifying specific *systems*. We will likely need to bring SC216 into this discussion – they are applying some of these concepts to security issues. For example, we will need to understand how to pass information of mixed DAL down the same pipe. We will also need to separate system security from network availability because the issue is not how to do end to end security, but rather how to handle disruption in *availability*.

Steve then explained the potential relationship between the revised MOPS content and the activities occurring in the related ARINC CSMIM committee. The original SC-236/WG96 messaging definition has morphed into an ARINC specification effort, strongly supported by Airbus and Boeing. The ARINC Cabin Secure Media Independent Messaging (CSMIM) specification is now being defined to support airframe managed centralized cabin network architectures. He noted that the existing approach of implementing centrally managed networks inherently requires a single network integrator working to a common design assurance level for all functions, and such networks are not compatible with safety-related functions unless designed to the highest design assurance level. The goal is to define CSMIM such that the messaging definition remains independent of a centralized architecture and centralized network services and is compatible with MOPS-defined Zero-Trust architectures. Steve describe the status of the ARINC effort toward producing this new standard and how the revised MOPS could reference it a possible MoC.

Agenda Item 5: Define the path forward

Steve asked the Committee if this approach, of splitting the existing MOPS into two separate documents to handle the network requirements independently from the RF requirements, would be an acceptable way to move forward given the uncertainties in the allowable WAIC power levels and the potential implications for WAIC viability. Anna noted that the MOPS this committee is developing will offer certification guidance for systems and applications that communicate across shared networks, including wireless media. It will include equipment hardware requirements necessary for individual network components to achieve secure communications across mixed-usage media. It is intended to be referenced by the FAA in a Technical Standard Order and by EASA in a European Technical Standard Order.

There was not consensus during the meeting on whether organizations participating in the Committee could support these changes. Members desired to discuss these proposed changes and provide a position prior to the next meeting.

Agenda Item 7: New Business

No new business was raised by the committee members.

Agenda Item 8: Review Plan for Next Meeting

Planning for the next meeting will occur by email.

Agenda Item 9: Review Action Items

- No specific actions were recorded other than for all committee members to consider the proposed changes to the ToR.

The meeting adjourned at 12:15 PM EDT.

Respectfully submitted by David Redman, Secretary SC-236.