Minutes of Meeting

EUROCAE WG-96 / RTCA SC-236 Plenary #3

Standards for Wireless Avionics Intra-Communication (WAIC) Systems

within 4200 - 4400 MHz

Date	*Tuesday November 28th – Friday December 1st , 2017*
Place	*D-50668 Cologne, Germany*
Venue	*EASA Headquarters*
Host	*EASA*
Contact Persons EUROCAE RTCA	*Sergiu Marzac* *<sergiu.marzac@eurocae.net>* *Phone: +33 1 40 92 79 31* *And* *Rebecca Morrison* rmorrison@rtca.org *+1 202-330-0654*

AGENDA

Tuesday November 28, 2017 9:00am to Friday December 1, 2017, 12:00pm.

1. Welcome/Administrative Duties
2. IPR / Membership Call-Out and Introductions
3. Acceptance of Meeting Minutes for the Second Joint Plenary of SC-236/WG-96
4. Review Plenary Agenda and Sub-working Group Schedule
5. Break into Sub-working Group meetings when plenary business complete
6. Reports of the Sub-Working Groups
7. Review of Special Committee Schedule
8. New Business Discussions
9. Review of Action Items
10. Plan for next meeting

11. Adjourn

Wednesday November 29, 2017 9:00 am-5:00 pm
  Continue with Plenary or Sub-working Group Meetings
Thursday November 30, 2017 9:00 am-5:00 pm
  Continue with Plenary or Sub-working Group Meetings
Friday December 1, 2017, 9:00 am – 12:00 pm
  Continue with Plenary or Sub-working Group Meetings

Attachments:
- Attachment A : Attendance List (Excel file)
- Attachment B : Action List (SC-236-WG96 WAIC) - status 2017-12
- Attachments C : Results of SWG sessions (are uploaded in RTCA shared website):
  - C1: Steven Rines SWG#2 final presentation (product of the SWG session).
  - C2: SWG#1: Working Paper for ICAO_Requirements_and_Procedures.doc

Appendices:
- Appendix 1: Notes and Result Report of SWG#2 (S. Rines)

Minutes of Meeting: November, 28th (start time 09:00)

Agenda Item 1 - Welcome

Welcome from EUROCAE Robin Davies (RD) (Chairman of WG-96). Chairman RTCA-SC236 Michael Franceschini (MRF) joint a bit later the day, and Secretary Peter Anders (PA) will join later on Thursday November 30.

Rebecca Morrison (RTCA) welcomes the group as well to the Plenary Meeting. Kevin Hallworth (EASA / host of the meeting) gave a short presentation on "housekeeping" and facts on EASA

The list of attendees is contained in Appendix 1.

Agenda Item 2 IPR / Membership Call-Out and Introductions

This meeting is a Plenary meeting (RTCA). It will be considered also as Joint Working Group meeting. Rebecca Morrison (RTCA) gave an introduction to the RTCA meeting rules and procedures. Paul Siegmund (FAA) officially opened the public meeting of SC-236.
Rebecca Morrison explained RTCA's "Proprietary Policy" and some general information on RTCA / EUROCAE membership modalities.
Rebecca referred to the standard presentation SC236_WG96_EUROCAE_RTCA.pdf – RTCA workspace:
http://workspace.rtca.org/apps/org/workgroup/sc236_standards_for_waic/documents.php?folder_id=5608

Agenda Item 3 - Acceptance of Meeting Minutes for the Second Joint Plenary of SC-236/WG-96
Minutes (MoM) of the second plenary meeting (College Station December 2016) were approved.

Agenda Item 4 – Review Plenary Agenda and Sub-working Group Schedule

The proposed agenda (see above) is accepted by the group. The list of action items (see Attachment B) has been reviewed. Remark, an update of the Status of Actions will be done on Friday, 1st Dec, agenda #9.

Agenda Item 5 Break into Sub-working Group meetings

Mike Franceschini explained the meeting schedule and made some final adjustments. All SWG leaders explained their expectations for the meeting
- SWG1: go through draft interim report content, get update on modelling assignments
- SWG2: go through Steve's presentation and seek agreement on open items
- SWG3: further evolve security architecture
- SWG4: finalization of discussion on FCC petition and functions.

A first session was done in joint way on 28.November (all subworking group together). On November 29th and 30th the SWGs split into two bigger sessions:
- Subworking Group# 1: to start elaborating RTCA interim report content.
- Subworking Group# 2: joint by members of SWG#3 and SWG#4.

Notes from the first joint session (28th Nov.):

Steven Rines gave a presentation on the discussion status SWG#2 (this presentation was used during later subworking discussion and elaborated further on – see Attachment C of this MoM). The presentation led to the discussion of a multitude of WAIC system aspects such as:
- Transmit function
- Receive function
- Security related functions
- Network management related function.

Notes from the session of SWG#1 (28th Nov. to 30th Nov):

For the objective of SWG#1 Thomas Meyerhoff presented the approach of first focusing on the "low coupling" scenarios. This approach was generally accepted.

The remaining time of this session was used for discussing the approach for deriving protection requirements and associated test procedures to cover WAIC-to-RA, WAIC-to-WAIC and RA-to-WAIC interference. Detailed discussion about protection criteria and test procedures for above cases was continued on 29th and 30th Nov in the Sessions of SWG#1.

Agenda Item 6 Reports of the Sub-Working Groups; Plenary wrap-up

Report from SWG#1 (Sanjay / Mike):

SWG-1 defined that WAIC components requires a test mode that will be used to verify system non-interference. On aircraft system test procedures will have to be included in MOPS chapter 4. Somewhere we have to describe how a WAIC system is installed, configured, tested, managed, maintained, shown to be secure, etc.

MOPS should include "typical equipment applications" and "operational goals." "Definitions and assumptions essential to proper understanding" should be included as well as "equipment tests and operational performance characteristics for equipment installations."

> Comment SHR: It looks like the MOPS should describe two classes of WAIC equipment: Simple WAIC and dynamically configurable WAIC components. These two classes should generally mirror the IEEE 802.15.4 descriptions for Reduced Function (RF) and Full Function (FF) devices.

Sections 2.3 and 2.4 should include equipment level tests. Section 4 should include aircraft level tests while performing the intended functions. Sections 2.3 and 2.4 may include details on features required in the equipment to allow security to be implemented. Section 4 may need to include tests to verify that system security is properly implemented across one or more applications.

The WAIC Control Plane shall be developed to the DAL of the highest DAL application that will use the network.

WAIC might be used to replace one set of wires in a redundant system but probably could not replace all wires in a redundant system due to common mode failure (e.g., jamming).

Other items discussed during SWG#1 session are:
- Differences between low coupling case.
- "dynamic conditions"
- Definition Test mode conditions
- "EIRP of radius x around A/C".
- IPL is too low for high coupling model xx dB.

One major Result that was elaborated during the SWG#1 session was the "Working Paper for ICAO Requirements and Procedures.docx" (see Attachment C2).

Report from SWG#2 &3 (Steve Rines):
The report of the joint sub working group session is given by Steve Rines. His summary is also included in the **Appendix 1.**

Report from SWG#4 (Paul Siegmund):
SWG-4 is writing the petition to the FCC to modify radio regulations to comply with the ITU resolution. (Basically, this changes radio allocations table to say "radio altimeters and WAIC." It may be appropriate to have participating companies submit justifications based on proposed applications.
ICAO SARPS will define system requirements for operations.

Agenda Item 7 Review of Special Committee Schedule

EUROCAE did align the schedule in EUROCAE WG-96 ToRs Schedule (initially target Mid 2018): Update to align RTCA Target March/2019.
(Which is optimistic –> Next meeting, the SC should consider to request postponing target date of MOPS).

Agenda Item 8 New Business Discussions

No point to discuss.

Agenda Item 9 Review of New Action Items

Refer to Attachment B Action List (SC-236-WG96 WAIC) - status 2017-12.

Agenda Item 10 Plan for next meeting

The next Joint plenary is planned **26th February – 2nd March in Washington, DC,** hosted by RTCA.
The next meetings after this one are planned:

- 22.05. - 26.05. Toulouse/France
- 27.08. - 30.08 Washington/DC (Draft ICAO white paper) or Beginning in October (Connecticut) or Japan
- 21st – 26 January 2019 Melbourne / USA.

The chairmen thanked participants for fruitful contributions and the host Kevin Hallworth of EASA.

Agenda item 11 Adjourn (Friday 13:00)

================ End of the fourth Day / End of Meeting ============================

Complied by Peter Anders   Secretary of SC-236/WG-96)
Approved by Michael Franceschini   *Co*-Chairmen of Joint SC-236/WG-96 (RTCA)
Approved by Robin Davies   *Co*-Chairmen of Joint SC-236/WG-96 (RTCA)

Appendix 1: Notes and Result Report of SWG#2 [1]

SWG2 – Essential task: Describe minimum node features to allow node to participate in WAIC; secondary task: Define minimum protocols required to support node participation.

Systems integrator is responsible for overall aircraft WAIC non-interference.

If a WAIC subnet is added to an aircraft that already has a WAIC Network onboard then the subnet will have to be integrated by the aircraft manufacturer to ensure the aircraft continues to meet non-interference criteria.

WAIC is not intended to operate in the PIES domain. Passenger use of a transmitting device in the WAIC spectrum is a criminal offense. Neither is passenger data intended to access or traverse a WAIC network.

Applications that aggregate and communicate cabin equipment status or perform maintenance functions over WAIC may be assumed to be operating in the AIS domain in support of regularity of flight.

For instance, cabin maintenance data that is properly encapsulated and constrained could potentially be delivered across a WAIC network shared with applications of higher criticality.

If a WAIC network is to be used by applications of multiple DALs then protection mechanisms will be required that ensure that errant or faulty behavior by lower DAL applications do not disrupt or inhibit higher DAL applications.

Whatever mechanism is used to protect application data flowing across the network will have to be developed to the highest DAL of the applications that will pass data over the WAIC network.

Multi-DAL protection mechanisms may best be accomplished in a common WAIC radio design (e.g., babbling node protection, listen-before-talk, data prioritization lanes, etc.).

Simple WAIC networks may not be capable of supporting multi-DAL data traffic.

SECURITY REQUIREMENT: If a WAIC network is to be used by applications of multiple security domains then the effects of a security breach to a lower security application shall not affect the confidentiality, integrity or availability of the network traffic associated with a higher security application.

[Still need to consider potential impacts of breach to authentication and non-repudiation of higher security applications.]

If there is a connection across WAIC to airline network infrastructure then it may be necessary to document WAIC of compliance with EU Network and Information Systems Directive for Critical Infrastructure. Specifying DO-355/356 compliance may be adequate to accomplish this.

SECURITY REQUIREMENT: The WAIC network shall maintain security logs in compliance with DO-356A and ED-203A.

[? Are common file formats/data structures defined in DO-356A and ED-203A? If not, do we need to define common structures in WAIC MOPS?

ARINC 852 provides optional guidance on interoperability requirements, data formats and log file contents to support security monitoring by airlines and operators.

SECURITY REQUIREMENT: Operators shall meet requirements of DO-355 for collection, delivery and review of security logs.

? What other information must be collected from WAIC?

MOPS should define the minimum requirements to allow compliant WAIC systems to be independently developed. ARINC specifications should be used to define interoperability.

Design intent is best captured in appendices.

End-to-end data security may be required depending on the application.

SWG-3 Task: Define the generic wireless threat model for use in the MOPS. (Refer to WOBAN process spec appendix G)

System integrator will integrate security from multiple WAIC suppliers.

Application developer should provide sufficient security details to enable the system integrator to perform system security assessment.

---

[1] These following notes were compiled by Steve Rines, and being copied in this MoM.

System integrator shall define how security is maintained for continued airworthiness for the operator (reference ED-204)

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS
ED-203A draft
Continued Airworthiness section 2.5
When a system is being developed and provided to an integrator as part of a development program, the Airworthiness Security Process suggests that the system provider should provide security instructions and guidance to the integrator. The System Provider should include the system-relevant information necessary for the Design Approval Holder (DAH) to develop the Security Instructions and Guidance for the Operator (see ED-204 / DO-355 for the information that should be considered). In addition, the System Provider should also provide conditions, limitations and procedures required to install and configure the provided equipment in secure condition.
NOTE: These considerations apply to all certifications; TC, ATC, STC, ASTC, and TSO.
The purpose of Continuing Airworthiness Security is to ensure that the aircraft continues to be protected from IUEI.

The main activities of Continuing Airworthiness Security from John Flores to everyone:

Security are to provide the instructions and guidance necessary to maintain the security posture of the aircraft as it was defined in the certification Logging section 6.1.2.
For further information, ARINC 852 provides optional guidance on interoperability requirements, data formats and log file contents to support security monitoring by airlines and operators.

We need to define the security threat here to justify the existence of the following derived requirements (SWG-3).
- If end-to-end application security is required then security shall be implemented at the application layer.
- Dynamically configurable WAIC components shall only be modifiable across a secure control plane. [Where do we define how secure?]

Discuss in full Plenary:

1. Interface definitions are not typically included in the MOPS –those are defined in ARINC characteristics. E.g., the VHF Comm MOPS defines the power level and channels but does not specify how the radio is tuned.

   The implication is that all WAIC form, fit, function, network management and other control details and interface control definitions (ICDs) should be documented in ARINC characteristics.
2. Should the MOPS define the RF modulation schemes? If not, where do they get defined?

   Wi-Fi ARINC specs define modulation.
   MF: We will define sensitivity and bit rate and performance within a interference environment.

MOPS normally define performance such as frequency range, wave form and that frequencies must be selectable in TBD steps.
MOPS must define what can be configured in a dynamically configurable WAIC node via control plane, not how it will be configured. The following elements may be configurable and reportable:
- Channel selection
- Channel width
- Modulation
- Sub-channel size (if applicable)
- Sub-channel selection (if applicable)
- Power level
- Node ID (location)
- Data rate

Configuration Control reportable elements:
- CAGE code
- Node hardware part number
- Node software part number
- Node service bulletin identifier(s)
- Serial number
- Security/Authentication parameters (TBD)

<u>from John Flores to everyone:</u>
> Logging
> Section 6.1.1 ED-203A
> Security notifications
> The design of the system should account for possible failures in security measures and the associated responses due to external attacks. In all cases, the safety of the aircraft should be designed into the system, such that safety is never compromised by a response to an attack. Failures of security measures should not be allowed to impede the communication of important systems, such as navigation and flight controls.

Security events that cause a safety effect could result in existing flightcrew alerting following the guidance provided by AC 25.1322-1 and other documents. No flightcrew alerting messages should be added specifically for security events.

Maintenance messages may be issued to give a fail/safe status and/or when a maintenance action may be necessary, in response to security events. The Minimum Equipment List, Aircraft Maintenance Manual, Line Maintenance Manual or other appropriate location should document the conditions (if any) under which the maintenance actions may be deferred, and for how long.

PS: Maintenance/Troubleshooting should go in MOPS section 4 or an appendix.
Advisory circular needs to be created as a companion to the MOPS.
In MOPS Section 4 recommend: The WAIC system or the using application should be able to report its operational status or performance degradation. (One implementation method to accomplish this would be for each WAIC node to periodically report its BITE results/fault information.)

WOBAN 3.4.4.1…

> *The Certification Applicant should be aware that, depending on the criticality of the WOBAN system and the associated applications, the implementation of an inherent monitoring system might be required to achieve continued airworthiness. It is expected that built-In monitoring functions will detect unacceptable performance degradations. In any case, based on the WOBAN System Integrator's proposal, the Certification Applicant should establish appropriate maintenance instructions to maintain airworthiness.*
> *It is highly recommended to include a Built-In-Test function into the WOBAN system which should be capable of measuring relevant performance metrics and detecting internal failures, storing them and making them available for instance as a maintenance inspection report. If this is technically impossible because an interface to the on-board maintenance reporting system is not foreseen, a dedicated system interface should be made available to provide the results of the Built-In-Test.*

Management of WAIC will probably have to be described in a MASP or an OSID (Operational Systems Interface Description). MASPs are usually used to generate an Advisory Circular for how to implement.
Alternately we will have to generate appendices for each of the topics that describe how WAIC should be managed.