RTCA Paper No. 074-24/SC216-150
EUR 105-24 WG72-176

St. Denis and Washington DC, 04/10/2024

EUROCAE WG-72 Meeting #73 / RTCA SC-216 Meeting #64 Joint Plenary

"Aeronautical Systems Security"

Date	***Monday – Friday 4-8 December 2023*** *09:00 – 17:00 MST / 17:00 – 23:00 CET* ***Friday 8th ends at 13:00 MST***
Place	***Honeywell Aerospace (and Virtual)***
Venue	***Honeywell Aerospace – Phoenix Deer Valley*** ***21111 N. 19th Ave.*** ***Phoenix, AZ 85027***
Hosted by	***RTCA/Honeywell Aerospace***

Points of contact: Javier Diana javier.diana@eurocae.net
Karan Hofmann khofmann@rtca.org

Attendance: (P – In Person / X – Remote)

Contact	Organization	DEC 4	DEC 5	DEC 6	DEC 7	DEC 8
Abbayu Libabu	ERAU				X	
Adam Patrick	Rolls Royce	X	X	X	X	
Alan Teyssier	FAA				X	
Alain Combes	Airbus	X	X		X	X
Ana Pasuca	IATA	X	X	X		
Andreas Henke	DLH	X	X	X	X	X
Andrew Drake	NetJets	P	P	P	P	P
Anup Raje	Honeywell	P	P	P	P	P
Ben Nagel	CyberBen	P	P	P	P	P
Bernard Margelin	Airbus		X			
Bill (William) Trussell	IFR Development	X				
Carlos Castro	ERAU				X	
Charles Sheehe	NASA	X		X	X	X
Cristian Bertoldi	Airbus	X		X	X	
Cyrille Rosay	EASA	P	P	P	P	P
David Aharon	Self				X	
David Harvie	ERAU	X	X	X	X	X
David Pierce	GE Aerospace	P	P	P	P	P
Davide Martini	EASA	P	P	P	P	P
Dj Balo	Netjets	X	X	X	X	X
Frédéric Heurtaux	Safran Group					X
Gabe Elkin	MIT			X	X	
Gilles Thales Descargues	Thales Group		X			
Hagop Kazarian	Bombardier	X	X	X	X	X
Hannes Alparslan	European Defense Agency (EDA)	X		X		X

Contact	Organization	DEC 4	DEC 5	DEC 6	DEC 7	DEC 8
Hiroyuki Shibahara	JCAB	P	P	P	P	P
Isidore Venetos	FAA		X	X	X	
James Ladd	Honeywell		P	P		
Jacub Cunat	EGIS Group					X
Javier Diana	Eurocae					X
Jayson Clifford	ERAU				X	
Jeff Burkey	FAA	X	X	X	X	X
Johannes Kramer	DLH	X	X	X	X	X
John Flores	FAA	X	X	X	X	X
John Peace	FAA				X	
Jose Romero-Mariona	Raytheon Technologies	X	X		X	X
Jonathan Lee	MIT - Lincoln Labs				X	
Kanwal Reen	Collins Aerospace	P	P	P	P	P
Karan Hofmann	RTCA	P	P	P	P	P
Keith Garfield	ERAU				X	
Ken Alexander	FAA			X		
Ken Kitamura	JCAB	P	P	P	P	P
Kevin Harnett	IOactive	X				X
Kevin Meier	Cessna Aircraft Company	X	X	X	X	X
Kris Milczewski	Lufthansa					X
Lee Howard	Honeywell	P	P	P	P	P
Ludovic Donnadieu	Airbus					X
Manon Gaudet	IATA	X	X			
Marcus Labay	FAA		X			
Marie Chantal Mouret	Airbus				X	
Mario Lenitz	Austro Control	X		X		X
Mariusz Pyzynski	IATA	X	X			X
Mark Kelley	Belcan	X	X	X	X	X
Marshall Gladding	Boeing	P	P	P	P	P
Martin Call	Boeing	X	X			
Matthieu Willm	Dassault Aviation	P	P	P	P	P
Michael Welch	FAA				X	
Mikaëla Ngamboé	Polytechnique				X	X
Mike McCartney	FAA	X	x	X	X	X
Mike Tumminelli	Gulfstream	X	X	X	X	X
Mila Obradovic	ECN	P	P	P	P	P
Minh Trang	Airbus		X			
Mitch Trope	Garmin	P	P	P	P	P
Myles Jalalian	FAA			X		
Nha Nguyen	Boeing			X		X
Nicolas Durandeau	EASA	X	X			X
Olivia Stella	SWA	P	P	P	P	P
Patrick Morrissey	Collins Aerospace	P	P	P	P	P
Paul Hoyt Nelson	NASA	X				
Peter Tsagaris	TC CA		X			X
Peter Wessel	DND GC CA		X			
Phil Watson	Panasonic	P	P	P	P	P
Philippe Dejean	Safran Group	X				X
Rob Hood	Astonautics	X	X	X	X	
Rosemberg Andre da Silva	ANAC-Brazil	X	X			X
Richard Nguyen	Boeing	X				
Sam Masri	Honeywell	P	P	P	P	P
Samantha LoPresti	FAA			X	X	X

Contact	Organization	DEC 4	DEC 5	DEC 6	DEC 7	DEC 8
Samer Falik	Faliksson	X				
Sarah Stern	Boeing	P	P	P	P	P
Seth Stewart	Pratt Whitney	X	X	X	X	X
Siobvan Nyikos	Boeing	P	P	P	P	P
Sean Crouse	ERAN				P	P
Sean hartzell	Boeing	X				
Stefan Schwindt	GE Aerospace	P	P	P	P	P
Tara Knight	SWA	X	X	X	X	
Ted Kalthoff	Archer Aviation	P	P	P	P	P
Ted Patmore	Delta	P	P	P	P	P
Tim Stelkens-Kobsch	DLR	X		X	X	
Thomas Parmer	FAA	P	P	P	P	P
Varun Khanna	FAA	P	P	P	P	P
Will Stephenson	MIT - Lincoln Labs				P	
William Trussell	IFR Development	X		X	X	X

**Post Meeting Note: The date at the top of the meeting minutes reflects the last date it was released, not the date that the meetings occurred.

WG 72 and SC-216 Plenary

Day 1, Monday 12-04-2023

- Sam Masri welcomed participants to Honeywell and shared facility safety information.
- Patrick M. and Siobvan N. opened the meeting, greeted participants and facilitated introductions of participants around the room and online.
- Karan Hofmann presented the RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, participation and membership policies.
- Siobvan N. presented the agenda
- Ted Kalthoff announced that Minutes from September 2023 meeting will be posted during the week and their formal approval is scheduled for Friday December 8th.

FAQ Document

- Ben Nagel presented collected topics for the new FAQ document. Collected topics included: layered defense diversity, isolation, and independence; COTS, TSO and legacy; SAL versus DAL; physical and operational security controls; secure coding standards; common criteria for compliance; supply chain security; and risk assessment comparability.
- FAA requires a security designation so that they look at systems that are developed to DAL E and have high SAL requirements. The idea is that DAL E software can fail, and no one cares. However, they need to properly function when they contain high SAL security measures. This should be added to the FAQ document topics.
- There is a need for clarifications on several topics within DO-356A to ensure consistent application of the standard.
- Karan is recommending we use an RTCA Report or EUROCAE ER document identifier instead of making this as a new DO/ED document.
- Varun and Karan have a concern about this document being a new means of compliance. We have to be careful about what is included in the change.
- If this update provides a new means of compliance, then it will need to be a DO-356BED-203B revision.
- Karan mentioned that we might want to just publish a DO-356A Change 1/ED-203A Change 1
- Siobvan suggested that we look at the following options:
    1. FAQ report
    2. 356B/203B revision
    3. FAQ report, then publish a 356A/203A Change 1 revision.
    4. New appendix in 356B/203B revision
- Options were discussed and the group decided on option 3. Siobvan took the action to propose an updated the TOR document for the group to review.
- Siobvan provided the following link for a folder that has files with FAQ doc options and topics: https://eurocae.sharepoint.com/sites/strato/8f4cae54-24d4-e611-80f2-5065f38bc5a1/9435b696-ad71-ee11-8179-000d3ab4bcd9/SitePages/Documents.aspx

SG4-ISMS

- Stefan reminded the group of the ISMS target document goal to produce a document that helps in providing means of compliance to Part-IS and future Information Security Manual regulations from ICAO
- Tara Knight/Southwest mentioned that the UK has separate ISMS regulations from the EU. Cyrille Rosay answered that the UK regulations are under consultation review now and that

they can be found at: https://consultations.caa.co.uk/cyber-security/uk-isms-regulation/user_uploads/rmt0019---isms-regulation---outline-structure-for-consultation-1.pdf

- Manon Gaudet/IATA mentioned that ICAO is also working on an Integrated Risk Management Systems outside TFP and CYSECP that will be coming soon.
- Siobvan provided a link for a folder that has the working copy of the ISMS document: https://eurocae.sharepoint.com/sites/strato/34fd374d-a1c8-e811-8154-e0071b66a0a1/d07cc886-a856-ed11-bba2-000d3adea767/SitePages/Documents.aspx
- Siobvan asked everyone involved to edit the document and send changes to Mark Kelly (editor)
- Siobvan reviewed chapters assignments and asked each volunteer group to review their section and make updates as appropriate
- Information Security Risk: "Distance to aircraft" text added to the working copy
- Supply Chain Security: Working on objectives, need to add to the working copy
- Safety Integration: Ch4 complete and ready
- Adam Patrick suggested that if we show harmony with other standards such as ICAO, IATA, ICF, and ACI, it will help ensure wider compliance
- Lots of discussion over bowties and newly added diagrams for Information Security Risk Assessment
- Stefan Schwindt presented a how risk is shown using the bowtie tool. In this tool SMS is used as an input. The risk is then classified and reported out to be mitigated.
- Stefan provided a link to a site that provides further details on the bow Tie risk management method: https://skybrary.aero/articles/bow-tie-risk-management-methodology
- Next step is to review text in working copy and provide comments/edits as appropriate
- Chapter leads need to provide text for sections assigned to topic/subgroup
- Since EUROCAE site is limited for editing, you can provide comments/edits to: Mark Kelley (editor) for incorporation into current working copy

Day 2, Tuesday 12-5-2023

SG6 DO 326B/ED-202B

- Sarah Stern presented a roadmap to submittal and a document release schedule.
- Dave Pierce reviewed changes made to the document with the group. Some editorial and suggested changes were made and addressed.
- Stefan shared the draft updated document with the group
- Martin Call voiced a concern that SC-216 standards are not prescriptive enough and allow too much interpretation.
- Dave Pierce explained that with these the modifications in the document, we want to be sure that the language is better than we had.
- Stefan mentioned that we need to update the text referencing the regulations to reference the specific paragraphs or the whole regulation rule to be consistent. He also mentioned that we need a sidebar with EASA and FAA to discuss Part 25 aircrafts with less than 19 passengers vs. all Part 25. *[(EASA does not make distinction for a large business jet with less than 19 passengers.) (For the FAA: The ASTM standards are an acceptable for all Part 23 aircraft. That includes 19 Pax or less Part 23 Class 4 airplanes.)]*
- Ben provided a link to where the draft document is posted: https://eurocae.sharepoint.com/sites/strato/8f4cae54-24d4-e611-80f2-5065f38bc5a1/b3053106-f232-ea11-a813-000d3ab118a3/SitePages/Documents.aspx
- Nicholas from EASA mentioned that he sent comments on the document. Patrick has the action to make necessary updates to address EASA's comments from Nicholas.

- Patrick discussed the update in 326A to introduce the SAL concept since it was not included in the Rev A document.
- Phil Watson/Panasonic asked if we could clarify the relation between SAL and DAL because we do not currently have a way to take credit for existing DAL requirements against SAL requirements.
- Martin Call added that if SAL is sufficient to show intended security function on its own, we should state that. And the phrase "encouraging the layering of security" seems to introduce a wish rather than a requirement.
- Stefan responded that it is ultimately a wish to do layering because the only time we are *required* to do defense in depth is for potentially Catastrophic events. We want to *encourage* as many layers as an applicant can put in but the exact number that is *required* is 2x for CAT and otherwise 1x.
- Martin responded that maybe we need to define "layer" of defense vs singular security measures. He added that many read the tables for SAL as applying to singular security measures.
- Ben added that the term Cyber was not introduced in the document. Dave suggested to use info sec instead of the word Cyber. Dave will make the global change.
- Phil W added that we should delete/change, “SAL commensurate with DAL” and replace “CVEs” with “vulnerabilities”, since there are vulnerabilities that are not CVEs.
- Rob Hood/Astronautics commented that doing an in-depth vulnerability analysis of all COTS would be very costly... especially with smaller organizations.
- Mark Kelley added that the term "Robustness Testing" is a DO-178C term. This may create some confusion that "we're already doing Robustness Testing".
- Stefan suggested saying that these tests verify the robustness of the security measures.
- Adam Patrick asked if a section on security validation is needed.
- Martin responded that there should be further discussion on security validation.
- ROSAY Cyrille responded that the purpose is to show that the system functions as intended and nothing else.
- Stefan responded that refutation encompasses testing and analysis activities such as security penetration testing, fuzzing, static and dynamic code analysis, formal proofs. This approach allows the system verifier to exercise the system with hundreds of thousands or even millions of tests as part of the verification activity. This approach (sometimes referred to as fuzzing or robustness testing) allows the system verifier to develop a high degree of confidence in the design of the system.
- Matthieu Willm/Dassault added that testing should identify design flaws that can be deeply buried in the code.
- Seth Stewart/PWC suggested that the FAQ for DO356A would be a great place to put all known standard examples of Refutation Verification.
- Dave took an action to develop a section on dynamic testing.
- Anup Raj/Honeywell commented that we should keep DO-326 document a process document and DO-356 as a method document.
- Stefan proposed that we need to update Figure 3-5. It should say DO-356.

Day 3, Wednesday 12-6-2023

<u>SG-5 DO-DSEC</u>

- DSEC presentation was led by Olivia Stella
- There was also a breakout session related to the DO-326B revision. The group made real time updates to the document based on previous day’s discussions.

- Olivia started with the scope and schedule for DSEC.
- Olivia reminded the group that the TOR goal is to “Generate a new document for publication addressing minimum standards for the generation, storage, and delivery of data, including Operational Flight Programs, sensitive maintenance data records and other security relevant data.” “The Standard on Aviation Data Security will provide specific technical details and timelines for the protection of data (executables, databases, data load activities, sensitive maintenance data, etc.) from malicious actors.” She added that we are focusing on a minimum viable product for this first draft.
- Anup provided updates from the sessions he led.
- Discussions focused on definition of data both to and from the aircraft.
- Point of reference brought up by Varun and Cyrille related to telemetry data.
- Need to make sure to separate into a different use case.
- Also make sure that unmanned data is segregated as well, since it is being dealt with in another working group as well.
- Cyrille mentioned that we need to take a look at the EASA/FAA/Boeing/Airbus white paper related to the criticality of the data.
- Large distinction of data 'to' the aircraft vs data 'from' the aircraft. Criticality point here is very important.
- Anup brought up privacy of data that was an important topic from Phil Watson
- Topic has been put on hold but needs to be addressed.
- Cyrille mentioned that this topic needs to be addressed due to GDPR.
- Not in scope but needs to be identified and may be addressed later.
- Kanwal mentioned that there may be other standards or rules that are related to data privacy that we do not want to supersede.
- Phil mentioned that there should be a note that you should reference the national laws related to your operational areas.
- Hannes Alparslan/EDA said that we need to focus on being agnostic.
- Hannes added that you can only achieve authenticity with tools like digital signatures where the certificates have been issued by a trusted Certification Authority. Integrity is a welcome “byproduct “of that. You can however ensure integrity without authenticity e.g. via SHA256.
- Ted K brought up the chain of custody conversation.
- This was the key focus for how to help ensure data security throughout the entire lifecycle of the data.
- Hannes mentioned that we need to identify the linkage with ISMS and how this data goes together.
- Use Case for Airborne Software and how to best protect the data was discussed in the afternoon.

Day 4, Thursday 12-7-2023

- Switched up the schedule this morning and started with ERAU's presentation on CSDS.
- MIT presented an FAA sponsored research project between ERAU and MIT LL
    - Trying to establish MOC.
    - Setup a test lab to start ingesting logs.
    - UC#1 started by taking in logs from day-to-day operations and started looking for anomalous behavior.
    - Defined two problem statements as part of their assessment.
    - Need a tool for identifying predetermined events.

    - Need a tool for analyzing data to determine if undefined events could also be malicious
    - High fidelity of detection of malicious logs
    - Still gathering logs data
    - MIT LL is the only ones who are allowed to touch the log data, which is from United Airlines
    - Olivia asked about the sharing of the results (not so much the log data itself)
    - Gabriel Elkin mentioned that any data gathered from the CSDC research program can only be shared at the discretion of the FAA.
    - Use Case #2 is a modification of the original use case.
    - Have a baseline aircraft profile that will be compared against now to help more quickly identify malicious or anomalous behaviors.
    - Alignment with DO-392/ED-206
    - Alignment with DO-392/ED-206 objectives
    - Possible future inclusions for DO-392/ED-206
- New presentation on CSDS for Supply Chain
- New presentation from Marie-Chantel Mouret from Airbus Helicopter
- Status from WG-112 for enhanced VTOL
- ED-305 = information security guidance for VTOL and collaborative systems
- Complementary methods for following AMC 20-42 with tailoring for VTOL.
- Tailoring of ED-202A with replacement of the aircraft and system scales to do a single process at the aircraft level for the whole VTOL perimeter will be required.
- Tailoring of ED-203A will also be required.
- Security risks focus on Haz and Cat
- Also tailoring of objectives related to COTS.
- Focusing on security assurance for SAL 3 protections
- Security assurance objectives in ED-203A remain for SAL 3
- Several recommendations for COTS components
- Have very descript selection criteria.
- Hardening of COTS components through security best practices or encapsulating them in security measures
- Testing, especially refutation testing
- Break
- Next presentation related to ISEM and ISMS integration.
- There will be two new chapters related to risk assessment => event management and current risk and security events
- These are updates to ED-206/DO-392 which will lead to a new ED-206A/DO-392A.
- Marshall Gladding started us out in the afternoon with a proposal for CVSS scoring for aircraft.
- This is to create aviation specific categories to any IT scoring systems.
- Relative scoring, not objective scoring
- Aviation standards should suggest baseline categories and a method for applying them to an organization.
- Areas that would be impacted in DO-392 have started to be identified.
- Second half of afternoon session broke apart to focus on wrapping up questions and changes for ISMS and ISEM before the official vote tomorrow on whether to put these documents out for OC/FRAC

Day 5, Friday 12-8-2023

- Siobvan presented meeting agenda.
- Decision was made to add FAQ document task to TOR task sheet as a report and an update to DO-356A Change 1/ED-203A Change 1 as a second addition.
- Minutes from the September 2023 plenary were reviewed and approved.
- Voting on a proposal to submit DO-326B/ED-203B update for FRAC/OC was conducted and approved. Majority of members voted yes. No one opposed it.
- Karan presented a slide to show the document timeline since we are going to FRAC/OC. To meet June release date, we need to give final clean document to RTCA by May 6. Then the doc will go to PMC in June. Council approval will be done electronically for a joint publication date.
- Karan suggested that we solve all non concurs before our next Plenary in April 2024.
- Javier from EUROCAE agreed with the RTCA process. Last day RTCA and EUROCAE working day this year is Dec 20th.
- Subgroup status was presented by each subgroup lead.
- SG-3 presented document progress status. Draft language has been proposed. The group had an action to add additional content for integration section in ISEM document. The document will then be circulated to internal teams for review and feedback.
- SG-3 presented a proposed CVSS scoring update to DO-392/ED-206. This will be incorporated into a draft for review.
- SG-4 presented subgroup status. Document high level objectives have been documented. The subgroup section leads have an action to update text in their sections.
- SG-5 presented document progress status.
- SG-6 had nothing new to present.
- Presentations providing other industry groups standards development effort status were provided. Here are some of the highlights.
    - SC-236/WG-96 Wireless Avionics Intra-Communication (WAIC) committee is working comment resolution within final MOPS DO-402/ED-319. Draft due from Member organizations by 11/16/23. Following final commentary closure, virtual plenary will close MOPS, address any potential member objections, and plan the future of the WAIC subcommittee.
    - SAE G-32 Cyber Physical Systems Security Committee had Ballot#2 out for JA6678 Cyber Physical Systems Security Software Assurance. Ballot closed October 4
    - SAE G-34/WG-114 AI/ML in Aviation Committee has a ballot out for AIR6987 Artificial Intelligence in Aeronautical System: Taxonomy. Ballot has November 21 due date.
- Regulatory Update -Japan: currently studying how to work with ICAO.
- Regulatory Update -EASA: There are ATM/ANS regulatory changes. Equipment supporting ATC should be subject to more stringent attestation methods (certification). Equipment supporting ATM/ANS should be subject to less stringent attestation methods (declaration of design compliance)
- Regulatory Update -FAA: Rulemaking just finished agency comments for the second time, on track for NPRM and AC should be out early next year. Rule will only be applicable to part 25, 33, 35 aircrafts. Part 23 may use ASTM document. Effectivity date not changed; compliance already started. Special condition has already provided the rule. Rule will not be equivalent to part IS. FAA may have other rule in place that could be like part IS. Part 33, 35 are making changes to their current rules.
- New Business: None.

- End