RTCA Paper No. 124-25/SC216-162
EUR 339-25 / WG72-188

St. Denis and Washington DC, 06/13/2025

EUROCAE WG-72 Meeting #80 / RTCA SC-216 Meeting #71 Joint Plenary **"Aeronautical Systems Security"**	
Plenary Date	***Friday 13 June*** ***09h00 – 13h00 PDT / 18h00 – 21h00 CEST***
Working Sessions	***Monday 09 June-Thursday 12 June, 2025*** ***09h00 – 17h00 PDT / 18h00 – 2h00 CEST***
Place	***Boeing (and Virtual)***
Venue	***Boeing*** ***Seattle-Washington***
Hosted by	***Boeing and RTCA***

Attendance:

Contact	Organization	13 June
Aaron Renshaw	American Airlines	
Abi Schmidt	UAL	X
Abinash Aryal	Southwest Airlines	
Adam Patrick	Rolls Royce	
Adam Smith	SWA	X
Adrian Waller	Thales Group	
Agnieszka Reinhardt	Liebherr Aerospace	X
Alain Combes	Airbus	X
Alan Teyssier	FAA	
Alessandro Oteri	Leonardo	
AmyClaire Brusch	ACI/NA	
Ana Pasuca	IATA	
Ana Santos	Embraer	
Aneesh Sankruth	Gulfstream	X
Andrea Cascio	Leonardo	
Andreas Henke	DLH	
Andrew Drake	NetJets	X
Andrew Kornecki	ERAU	
Aneesh Sankruth	Gulfstream	
Angeliki Karakoliou	EASA	
Anna Guegan	EUROCAE	X
Anup Raje	Honeywell	X
Arthur Pang	Boeing	
Barbara Clark	FAA	
Ben Nagel	CyberBen	X
Bernard Margelin	Airbus	
Bill (William) Trussell	IFR Development	
Billy Ogunsola	UK CAA	
Britney Boler	Southwest Airlines	
Cameron Wright	Southwest Airlines	
Carl Schuett	Southwest Airlines	
Cecil Deleon	Southwest Airlines	
Charles Sheehe	NASA	
Chris Gorton	UK CAA	
Chris Kendrick	FAA-AFS	
Chris MacMullin	CA Dept of National Defense	
Christopher Terrington	Collins Aerospace	
Claudio H	Lilium	
Cristian Bertoldi	Airbus	
Cyrille Rosay	EASA	
Dan Diessner	ERAU	
Daniel Nguyen	Boeing	X
Daniel Salter	UK CAA	X

David Chen	FAA	
David Harvie	ERAU	X
David Pierce	GE Aerospace	
Davide Martini	EASA	X
Deepak Kamath	FAA	
Emerson Luiz Cunha	EMBRAER	
Esha Vasdev	CA Dept of National Defense	
Fabian Cavenne	Thales Group	
Felix Meier-Hedde	Airbus	
Filippo Tomasello	EuroUSC Italia	
Florin Grafu	Romanian Air Traffic Services	X
Francois Triboulet	EASA	
Frédéric Heurtaux	Safran Group	X
Gabriel Elkin	MIT-LL	
Garcia-Blanco Castro Borja	EASA	
Garv Stephenson	Wisk	
George Chang	Boeing	
Gilles Thales Descargues	Thales Group	
Gregg Slade	Leonardo	
Hagop Kazarian	Bombardier	
Hannes Alparslan	EDA	
Ian Coaker	BAE	
Igor Hoffman	UAL	
Isaac Lee	Southwest Airlines	
Isaac Rodriguez	Wisk	
Isidore Venetos	FAA	
Ivan Padilla Muro	UPM Madrid	
J.P. DeKruiff	IOActive Cybersecurity	
Jakub Cunat	Egis Group	X
Jason Schoenbeck	Collins Aerospace	
Javier Diana	EUROCAE	
Jean-Paul Moreaux	EASA	
Jeff Burkey	FAA	
Jens Hennig	GAMA	
Jeroen Tuijp	Netherlands Aerospace Center	
Joe Reisinger	Astronautics	X
Johannes Goebel	EASA	
Johannes Kramer	Lufthansa	
Johannes vanHoudt	FAA	
John Craig - Shift5	Shift5	
John Flores	FAA	
John Peace	FAA	
Jonathan Lee (MIT LL)	MIT LL	
Jose M. Fernandez	Polytechnique	
Judicael Gros-Desirs	Airbus	X

Kamaran Evans	RTX	
Kanwal Reen	Collins Aerospace	
Karan Hofmann	RTCA	
Katoh Atsushi	Japan JAMSS Company	X
Ken Alexander	FAA	
Ken Kitamura	JCAB	X
Ken Natividad	Southwest Airlines	
Kevin Harnett	IOActive Cybersecurity	
Kevin Meier	Textron	X
Kristof Lamont	Euro Control	
Laurent Leonardon	Collins Aerospace	
Lawrence Baker	NCC	
Lee Howard	Honeywell	X
Lillian Baker	Boeing	X
Lindsay Rabinko	Triumph Group	X
Logan Cummings	GE Aerospace	X
Lucas Garcia	Embraer	
Ludovic Donnadieu	Airbus	
Luigi Marotta	Crisalion	
Luis Lozano	Ineco	
Manon Gaudet	IATA	
Marc Lord	CA Dept of National Defense	
Marcos Ramos	Embraer	
Marcus Labay	FAA	
Marcus Session	ACI/NA	
Marie-Chantal Mouret	Airbus	
Mario Lenitz	Austro Control	
Mariusz Pyzynski	IATA	
Mark Bucko	Boeing	
Mark Hingsbergen	GE Aerospace	
Mark Kelley	Belcan	X
Marshall Gladding	Boeing	X
Martin Call	Boeing	
Marty Reynolds	A4A	
Matthieu Willm	Dassault Aviation	X
Michael Vanguardia	Boeing	
Michael W Davis	FAA	
Michael Welch	FAA	
Mickael Sabelle	Collins Aerospace	
Mikaëla Ngamboé	Polytechnique Montreal	
Mike Goodfellow	ICAO	
Mike McCartney	FAA	X
Mike Noorman	GE Aerospace	
Mike Shalvey	Southwest Airlines	
Mike Tumminelli	Gulfstream	

Mila Obradovic	CA Dept of National Defense	
Milton Santos	EMBRAER	
Minh Trang	Airbus	
Mitch Trope	Garmin	X
Nha Nguyen	Boeing	X
Nicolas Durandeau	EASA	X
Nikita Johnson	Rolls Royce	X
Niv Siva	UK CAA	
Olivia Stella	Southwest Airlines	X
Pamela Davis	Southwest Airlines	
Prachi Shekhar	EGIS Group	
Patrick McTernen	Shift5	X
Patrick Morrissey	Collins Aerospace	X
Peter McNeely	Astronautics	X
Peter Tsagaris	TCCA	
Phil Watson	Panasonic	X
Phil Windust	FAA	
Philippe Dejean	Safran Group	
Pieter Wessel	CA Dept of National Defense	
Prachi Shekhar	EGIS Group	
Raphael Blaize	Thales Group	
Rebecca Morrison	RTCA	X
Rebecca Roberts	Collins	
Renuka Chitikesi	Honeywell	
Richard Nguyen	Boeing	
Rob Segers	FAA	X
Roland Olivier	Boeing	
Romuald Salgues	Airbus Helicopter	
Rosemberg Andre da Silva	ANAC-Brazil	
Sam Masri	Honeywell	X
Sanjiv Pimple	Panasonic	
Sarah Stern	Boeing	X
Seth Stewart	Pratt & Whitney Canada	
Shane Chen	Aviage Systems	
Siobvan Nyikos	Boeing	X
Sparpano Daniele	Leonardo	
Stefan Schwindt	GE Aerospace	X
Stephen Van Trees	FAA	
Tara Knight	Southwest Airlines	
Ted Kalthoff	Archer Aviation	X
Ted Patmore	Delta	X
Theresa Adams	Pratt & Whitney	
Thomas Parmer	FAA	
Thuan T Nguyen	FAA	X
Tim Stelkens-Kobsch	DLR	

Timo Warns	Airbus	
Tony Baghai	University of Washington	X
Valerio Senni	Collins Aerospace	
Varun Khanna	FAA	X
Viana Tavares	Embraer	
Vic Patel	FAA	
Xylene Gonzalez	Pelayo	X
Yutaka Ikeda	Japan JAMSS co	X

Day 1 Monday 06-09-2025

SC-216 & WG 72

- Siobvan welcomed the group to Boeing and provided facility safety information.
- Siobvan presented the agenda and facilitated introductions of participants around the room and online.

Regulatory updates:

- FAA-Varun: Rulemaking efforts are on track to publish in Jan 26.Thuan will be taking over the government representative role on the committee after Varun retires.
- FAA-Phil Windust. FAA,: Rule making committee ARC is included in the FAA reauthorization bill. FAA cyber charter was signed by the FAA administrator. Phil Windust will be ARC co chair. Committee kickoff meeting Tuesday June 17th. Tasks will be divided to working groups,
- EASA-Part-IS: Update of the GMs: Comments received are currently being reviewed, with the final publication expected in July.
- A Part-IS workshop is scheduled for June 25th and 26th.
- A draft document titled "Mapping of EU cybersecurity rules applicable to the aviation sector" is available. Document includes a mapping of AVSEC, Part-IS, and NIS2.
- EASA-Product Certification: CS ETSO Amendment 18: Set to be released, with Subpart A focusing on information security in alignment with safety and development assurance, although there are no fundamental changes.
- AMC 20-42 Revision: Ongoing, with no planned release date. This will recognize the latest standards (ED-202B, ED-305, ASTM F3532-25, ED-206) and includes guidance for change assessment based on ED-202B.
- EASA Cyber Guidance for Drones: Ongoing development of cyber guidance for SC Light UAS for drones, in addition to existing guidance.
- UK CAA; Chris: we hope to continue discussions. We are trying to get cyber on the agenda for many working groups. Big focus on supply chain. UK authorities are publishing a guideline document for drone operators

Next meeting dates and places:

- September 22-26 at Austro Control in Vienna, Austria (original dates)- PMC September 26 – got an exception-Sound check completed
- Panasonic successfully passed the RTCA sound check, making it a favorable venue for a committee meeting.
- RTCA still needs to review and approve the proposed meeting locations, and the last RTCA visit was in June 2024.
- Options for Meetings:
- Option 1: Schedule the December 2025 meeting at Panasonic, with all US meetings in 2026 to be held at RTCA.

- Option 2: Hold the December 2025 meeting at RTCA and request that one of the 2026 meeting locations be at Panasonic (with the other being RTCA).
- The leadership team recommends Option 2 as it is more balanced and likely to gain approval.
- The following proposal was made for 2026:
- Q1: March/April 2026 - RTCA in WDC or Panasonic in Irvine, CA
- Q2: June 2026-EUROCAE in Paris since it's been a couple years since we've been to EUROCAE
- Q3: September/October 2026-RTCA in WDC or Panasonic in Irvine, CA
- Q4: December 2026-EASA in Cologne
- Cost of going to meetings was discussed and it was pointed out that participation in expensive locations like DC may reduce participation. RTCA policies were cited and should be used.

DO-355B/ED-204B update:

- Olivia presented the topic of updating DO-355B / ED-204B and discussed how air operators receive airworthiness requirements as well as the impact of these requirements. Olivia discussed the scope of updates and needed resources.
- FAA's OpSpec D301 outlines airworthiness requirements related to cybersecurity vulnerabilities due to unauthorized access to aircraft systems.
- The Flight Standards Information System requires operators to implement an Aircraft Network Security Program (ANSP) for connected aircraft.
- Compliance with guidance from design approval holders (DAH) is mandatory for continued airworthiness certification by the FAA.
- EASA mandates that aircraft operators develop and maintain security programs specific to their operations.
- Current guidance aims to protect electronic systems and prevent unauthorized interference.
- Various international regulations exist, whereby entities like the UK CAA and Transport Canada align with EASA and FAA standards.
- Introduction of Part IS for information security management systems (ISMS) that include ground systems, irrespective of whether the aircraft has special conditions.
- Development of a robust Aircraft Information Security Program (AISP) based on DAH guidance.
- Management of continuing airworthiness, system definitions within AISP scope, and staffing for risk assessment and incident response.
- Evidence of compliance through monitoring aircraft log files.
- Plans for subgroup leadership completion and development of a timeline for the DO-355B publication.
- Discussion on the need for additional guidance and integration with established standards, highlighting perceived gaps in the existing documentation.
- Emphasis on missing digital signatures and subsequent actions stemming from industry conferences on ARINC 851.
- AC 119-1 A web location was provided: AC 119-1A - Operational Authorization of Aircraft Network Security Program
- Anup raised a concern about whether the SSIG information provided to the OEM by Honeywell is accessible to operators, to which Olivia responded that it does not reach them and tends to get lost within the system.
- Stefan emphasized the importance of being specific regarding the actions operators can take to secure the aircraft system, indicating that detailed software design information is not necessary.
- Varun recalled the Alaska Air MD-80 accident and stated that operators should be prohibited from making changes—such as lubricant modifications—without first

consulting their OEM.

- Stefan referenced that these security concerns are generally addressed in aviation regulations like Part 21, 145, 121, and 135.
- Lee suggested incorporating security guidance directly into the maintenance manual for enhanced operator awareness.
- Nicolas argued that OEMs should restrict communications to operators more effectively, suggesting that many manufacturers do not provide sufficient instructions due to minimal reliance on such protocols.
- Boeing mentioned that many assumptions made about operators during product development have not been validated, but steps are being taken to correct this.
- Varun proposed that operators should unite in requesting clearer cyber security instructions from OEMs.
- Stefan touched on compliance with European airworthiness requirements as part of the broader discussion on improving security measures.
- Olivia was assigned an Action to collaborate with Stefan on creating an informative diagram following the end of the discussion.
- Varun predicted that the FAA will probably produce a version of part IS that will bridge requirements between Europe and the US.
- Alessandro inquired whether ED204B would explicitly reference ED206, prompting Stefan to confirm that ED204B does refer to ED206.
- Stefan noted that the NPRM will differentiate between ICA and other guidelines, and that the ANSP provides the framework for operators' plans, indicating potential overlaps with ED204.
- Varun pointed out that currently, such overlaps are primarily a concern in Europe.
- Aneesh expressed that the distinction between where ED-204/A Guidance ends and Part IS begins is becoming increasingly unclear, highlighting that ED204 includes guidance on developing ICA, which may encompass operational security measures.
- Varun mentioned the benefits of examining changes to legacy aircraft to assess risks and stated that special conditions apply when changes impact the aircraft and create new entry points.
- A member asked whether the payment system was part of the discussion, with clarification made that it is a DAL E system and does not impact safety.
- Ben noted that while the network infrastructure won't change, controlling and monitoring access points is the key concern.
- Stefan suggested renaming the focus to "aircraft attack surface" for clarity.
- Anup highlighted that current documents fail to address databases adequately, recommending the addition of clarifications for better guidance.
- Siobvan emphasized the need for targeted sharing rather than an overwhelming flow of information.
- Stefan pointed out that ED204A/DO355A briefly mentions databases, but more clarity may be needed.
- Judicael stated that focusing on "AISP contribution to global risk management" should be acceptable in risk assessment efforts.
- Aneesh clarified that part of the issue relates to securely handling sensitive security information to avoid consequences from unauthorized disclosure, emphasizing the importance of clearly communicating such reasoning to operators.
- Stefan warned that operators acting based on an SBOM might risk airworthiness or unintended responsibilities due to lack of understanding.
- Nicolas noted that the ASOG content described in ED-202B is limited and should be expanded to better serve operator needs. Aneesh added that ED204A outlines ASOG requirements per topic.
- A concern was raised about a GSE (Ground Support Equipment) interacting with the aircraft's data loader but not meeting DO-355 requirements, pointing to a lack of

communication between OEMs, operators, and GSE providers.

- Ben referred to links with future ED206 revision and questioned how EU airlines could be involved, particularly concerning risk assessment overlaps (Part-IS).
- Ben pointed out that reliance solely on ED355/ED204 for requirements within ASOG and the Security Handbook is insufficient.
- Nicolas argued that fully copying ED-204A in the ASOG implementation is incorrect.
- Siobvan outlined process priorities and allocated time for logistics discussions.
- Ted volunteered as secretary, and Mark tentatively took on the Editor role.
- Ben advocated for involving an EU airline in discussions, offering himself as a liaison
- Stefan expressed interest in engaging Eurocae members, noting Finnair is not yet a member and wishing for their participation.
- Abi Schmidt volunteered to serve as SME for GSE/GSIS matters.
- Anup discussed the letter received from airlines regarding the verification of signatures from the source. Explained that OEMs are beginning to sign artifacts, integrating these into operator processes, and inquired about the capability of supplier tools to verify signatures. Mentioned the need for a universal tool for verifying signatures, related to software data loading.
- Aneesh questioned why A835 does not assume the responsibility for ensuring interoperability, instead of relying on DO-355.
- Stefan clarified that A835 is not an AMC whereas DO-355 is. Highlighted that DO-355 cannot specify the use of a format for signing, but can specify relevant and applicable information.

Day 2 Tuesday 06-10-2025
SG-6

- Sarah reviewed comments and proposed responses for ED-203A Change 1 (DO-356A Change 1).
- Stefan and Ben raised concerns regarding unidirectional Ethernet, clarifying its reliance on configuration settings and suggesting inclusion in FAQs.
- Stefan discussed differences between EASA and FAA handling of circuit board assemblies and the potential implications.
- Philip and Ted contributed to the conversation on hardware definitions, emphasizing detailed clarification between simple and complex hardware, and their appropriate regulatory applications.
- Martin suggested defining hardware for cybersecurity as anything processing digital data, while Aneesh proposed adding AEH definitions to ensure consistent use throughout the document.
- A consensus emerged to address the need for uniformity in hardware definitions but determined that changes would be more appropriate for revision B, not Change 1, due to their complexity and impact.
- Stefan emphasized distinguishing between security measures and detection mechanisms, with agreement from others that security logging is not a preventive security measure but supports post-event forensic analysis.
- Matthieu Willm proposed revising the discussion on security logging and adding clarification around industry standards like ARINC 645, ARINC 827, and ARINC 835 for secure data loading to ensure alignment across stakeholders.
- Stefan and others highlighted the need for cryptographic integrity verification for loadable software, noting that older equipment with hardware limitations would require offboard integrity checks.
- Nicolas noted that compensating technical measures might be necessary in cases where load signing is not immediately feasible.

- Philip and Martin proposed emphasizing clear language in Section 5.6.2 to differentiate between guiding recommendations and mandatory requirements.
- Lee noted the importance of providing distinct guidance for fielded (legacy) equipment versus new equipment, acknowledging the differing capabilities for cryptographic self-checking.
- Discussions concluded with agreement to refine wording, balance flexibility and standardization, and improve Section 5.6.2 with clearer principles related to integrity and authenticity verification for loadable software.
- Sarah suggested removing Change 1 from the TOR
- Siobvan suggested fixing errors via an errata by stripping out non-consensus items, with the understanding that Change 1 is to be removed and Revision B is forthcoming.
- Ben inquired about any duplicate comments in the NC/H discussions to reduce workload. Lillian confirmed that some duplicates existed in previously discussed sections.
- Sarah noted that some sections contained many NCs while others did not, indicating overlapping NCs.
- Stefan noted that COTS are under scrutiny regarding meeting cyber requirements.
- Gilles and others agreed that supply chain management should be linked to vulnerability management and indicated it ought to be reflected in the FAQ document.
- Stefan clarified that vulnerability identification is part of certification while vulnerability management applies to in-service products.
- There was a discussion on Security Management Plan (SMP): The group acknowledged the lack of a defined SMP and emphasized that there may be value in including a definition.
- A consensus was reached that while NPRM isn't out yet, the objectives should ensure vulnerabilities impacting safety are monitored.
- Martin suggested separating the vulnerability management requirements for certification from those needed for continued airworthiness.

Day 3 Wednesday 06-11-2025

- Andrew welcomed participants to SG-3 ISEM
- Andrew presented an agenda for the day that included document revision review, progress discussions, proposed going forward plan and timeline
- The group had discussions around adding specific objectives and establishing timelines related to vulnerability management. The objective is to implement a structured approach that includes response measures tailored to the different parts of the aviation industry while acknowledging the uncertainties inherent in evolving situations.
- The group focused on defining actionable objectives with timelines, fostering improvements in responses to vulnerabilities, and addressing the need for performance metrics to track progress effectively.
- An appendix was added to talk about PSDS
- Andrew presented the updated TOR timelines
- Stefan suggested that event over-reporting to authorities is okay if it is acceptable to withdraw reports when incidents are later found to be under the safety reporting thresholds through more detailed analysis.. Stefan proposed using risk measurement to aid reporting.
- Sarah emphasized the need for alignment between special conditions and the 90-day log collection and storage requirement.
- Lee suggested taking an objective-based approach for initial investigations, ensuring prescriptive reporting timelines similar to safety processes.
- Olivia proposed the creation of distinct sections for aircraft and ground/OT/IT.
- Andrew shared a draft outlining needed updates.

- Alain discussed the significance of safety distance definitions for risk assessment
- Andrew reviewed document changes, proposing to move the section “Inventory of security measures mitigating risks for aviation safety” to an appendix, which received agreement from others.
- Siobvan noted that the ISMS report has completed the RAC process, indicating limitations on editing unless issues arise during comment resolution.
- Stefan stressed that organizations may implement various arrangements to ensure necessary safety management functions align with their needs.
- Logan suggested simplifying sentences relating to security measures to avoid contradictions.
- Ted highlighted the intersection of physical security and cybersecurity, particularly concerning access controls.
- Patrick raised questions about handling devices that cannot run antivirus tools by design.
- Stefan pointed out that the reliance on a human is unavoidable in security measures.
- Matthieu suggested linking triage efforts with the vulnerability management strategy, noting that not all vulnerabilities will be assessed. He mentioned that less critical vulnerabilities in IT environments often just receive patches.
- Andrew discussed the "preparing incident management" section asking for group feedback.

Day 4 Thursday 06-12-2025

- Patrick opened the meeting by asking for clarification from airlines to help the group understand DO-355 issues airlines are facing with cyber security regulators. The group discussed potentially developing presentations by the airlines, the OEMs and avionics developers.
- Rebecca-RTCA added that chairs may invite experts for limited participation in working meetings

<u>Transitioning to ISMS</u>

- Siobvan presented the status of the ISMS document. Siobvan presented the SC-216/WG-72 SG4 AVIATION ISMS presentation slides, walking the group through the agenda for the day. Siobvan presented the stats on the ER-ISMS comments and where we stand going into today:

    - Pre-RAC Comments = 115
    - RAC Comment Count = 637
    - NC’s – 21
    - High – 157
    - Medium – 160
    - Low – 109
    - Editorial – 190
    - Total comments addressed = 751
    - One Medium rated comment remains open to address. The group discussed the open comment and the proposed solution was presented.
- Siobvan proposed the deletion of Principle 9.
- Mark added that the issue was discussed with Davide and suggested further evaluation of the principle.
- Nikita expressed concerns regarding the immaturity of the subject matter related to certified products. Noted potential issues in defining credit for certified products and suggested it may be better to omit the principle to avoid confusion.

- Nicolas discussed the complexity of limiting certification to a product. He noted the need for clear wording, emphasizing that certified products should be recognized in the scope of compliance with Part IS.
- Mario highlighted the distinction between ISMS and product certifications. Stressed that compliance with Part IS does not guarantee product security. Noted that certified products can contribute positively, depending on certification criteria.
- Nikita cautioned against double accounting. Mentioned that risk assessments conducted during product certification should be accounted for accurately.
- Mark presented a new wording proposal from Stefan.
- Mario questioned the accuracy of the initial wording and suggested rephrasing.
- Siobvan reminded participants that the material discussed is for a report rather than a comprehensive document.
- Lilian noted the presence of duplicates in the bullet points and recommended using "should" instead of "may" in the concluding sentence regarding airworthiness considerations.
- The group finally agreed to delete principal 9 as initially proposed.
- Olivia presented the idea of using Jira to track parking lot items. The group decided to consult with Eurocae and RTCA about the use of the JIRA tool.
- SG6 leadership updates were discussed and finalized
    - Co-Lead (RTCA): Lily Baker
    - Co-Lead (EUROCAE): Stefan Schwindt
    - Secretary (RTCA): Lee Howard
    - Secretary (EUROCAE): Jakub Cunat
    - Scribe/Writer: Mark Kelley
    - Content Contributor: Rob Segers
    - SMEs: As identified in subgroups

Day 5 Friday 06-13-2025-Plenary

- Rebecca Morrison and Anna Guégan presented the RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, recording, AI use, participation and membership policies. Rebecca included an export compliance policy slide.
- Stefan asked for a copy of slides/template for the new branding. Anna indicated that the information is posted to the server, workplace. [https://eurocaeapp.sharepoint.com/:p:/r/sites/eurosky/EUROCAE%20Toolbox%20Documents/RTCA_EUROCAE_Opening_Slides%202025%20July.pptx?d=wd363e295ff7c4e95bbd7bde526892044&csf=1&web=1&e=I2YEuO (However, while the first slide has a RTCA/EUROCAE co-branding and it has all the pre-amble slides for a plenary, it does not have co-branded working slides. Action: Template should be updated)]
- Anna presented a slide that listed several cyber security related training classes that are offered by Eurocae.
- Meeting minutes from the March 2025 plenary were approved
- Siobvan asked for a volunteer for the open secretary position for Eurocae' s WG 72. Anup volunteered to take the open position. Siobvan took the Action to send an email to Anna to indicate Anup's nomination for the position.
- Siobvan presented and discussed the SC-216 future 2025 and 2026 meeting plans:

    - 2025
    - September 22-26 at Austro Control in Vienna, Austria (original dates)
        - Sound check completed
    - December 8-12

        - RTCA in WDC
    - 2026
    - Q1: March/April 2026
        - Week of March 2nd
        - RTCA in WDC or at Panasonic Irvine CA
    - Q2: June 2026
        - Week of June 1st
        - Eurocae Paris
    - Q3: September/October 2026
        - Target September 14 or 21
        - RTCA in WDC or at Panasonic Irvine CA
    - Q4: December 2026
        - EASA in Cologne
        - Week of December 7th

NOTE: The 2026 meetings dates and places discussed in the June plenary have evolved and will be finalized at the September plenary.

- Leadership indicated that this schedule swap will be tried in 2026. The meeting schedule will be changed back if the swap did not work.
- Leadership encouraged operators, airlines and airport organizations to host committee meetings to promote engagement. Promoting tours of facilities would be helpful.
- Olivia requested using an operator visit to host a meeting to facilitate for a better understanding of operations at the operator's site
- Ben suggested involving LH on the EU side for support.
- Philip proposed the idea of a SOC tour.
- Rebecca indicated that this presents a good opportunity for the leadership team to discuss alternative locations for meetings.
- Abi Schmidt mentioned she would reach out to United leadership about hosting meetings at IAH, ORD, or LAX.
- Ted mentioned Delta as a potential hosting option, pending audio capability checks.
- Ben raised concerns regarding GPS spoofing
- Olivia suggested possibly having two operators lined up in 2026 for DO-355 support.
- The group debated potential dates for 2026 meetings, with a suggestion to limit to three face-to-face meetings annually.
- Rebecca mentioned that PMC meetings are scheduled one year in advance to prevent conflicts.
- Daniel Salter pointed out the usual timing for the ICAO CYSEC panel in early June.
- Rebecca indicated the week of the 14th is likely reserved for PMC.

SUBGROUP STATUS

- SG-4 ISMS Report Status
- Comment Closure Status: Complete!
- Parking Lot Item(s): ISMS for Aviation Organizations industry standard
- Vote – Are we ready for publication? The group voted with YES
- Next Steps: Clean up process to ensure report has accurate membership list, correct formatting for RTCA and EUROCAE, etc.
- Not ready in time for PMC, but might be possible to get an out of cycle approval if complete prior to PMC June 26 – contact your PMC reps
- Siobvan and Patrick can verbalize this while DSEC report is presented to PMC
- After the report is published, Siobvan will step down as RTCA SG4 Lead
- Siobvan asked for a volunteer to lead SG4

- The next projected task of SG4 will be an ISMS for Aviation Organizations industry standard (normative unless otherwise stated for certain sections)
- Below are the stats on the ER-ISMS comments and where we stand going into today.

    - Pre-RAC Comments = 115
    - RAC Comment Count = 637
    - NC's – 21
    - High – 157
    - Medium – 160
    - Low – 109
    - Editorial – 190
    - Total comments addressed = 751

SG-3

- SG-3 ISEM Report Status
- Andrew presented the subgroup status and updated document timelines. Updates were completed to sections 3.3 for ISMS and ISEM integration and section 3.4 for guidance on vulnerability management. Andrew reviewed content for planned updates and timelines.
- Andrew updated document on the Eurocae server.
- Andrew discussed timeline for the document. The big decision is on being ready to publish in September.
- The decision on whether to proceed with Rev A document or delay for further refinement was discussed.
- Key Concern raised was text misalignment with ISMS
- Stefan recommended delaying to ensure content has value and maturity.
- Rebecca noted PMC will follow the committee's decision.
- Alain suggested recalibrating the schedule and setting a new publication date due to readiness concerns.

SG-5 DSEC

- SG-5 DSEC Report Status
- Anup suggested keeping the SG 5 number for DSEC because the document will be updated.

SG-6:

- SG-6 FAQ Report Status
- Nikita presented the subgroup status and updated document timelines
- The group will continue to resolve NCs and High comments
- The group voted to remove change 1 from TOR
- Rebecca Morrison from RTCA recommended to do a virtual plenary in August in preparation for a September PMC.

SG-8:

- SG-8 DO-355B Document Update Status
- Olivia presented applicable TOR wording and a definition of envisioned deliverable
- Olivia discussed AISP/ANSP and reviewed lessons learned from the existing DO-355.
- Olivia discussed the scope of the new revision and needed resources
- Looking for volunteers to confirm their interest
- Rebecca added that she needs to coordinate with Anna about the subgroup name

Next topic: PARKING LOT ITEMS-TO DO LIST

- Future parking lot items are important

- Siobvan expressed the need for a tool to capture future work
- Committee members are to maintain a list of glossary items that have been added until we can update ER-013A.
- Rebecca mentioned that RTCA has insights on how other groups track similar items and expressed willingness to discuss the possible use of tools for this purpose.
- Aneesh suggested that since EUROCAE uses SharePoint, they might apply restrictions on files such as requiring a "check out" and "check in" process.
- Rebecca highlighted that the backend of AerOpus is also SharePoint, but there is uncertainty about which tools are configured for multiple organization access.
- Rebecca will remind Siobvan and Patrick about a survey they received to provide feedback on their needs for collaboration tools.
- Patrick discussed his experience at his company tracking PR log.

Next topic- Refutation and Robustness testing

- Daniel Nguyen presented slides on Refutation and Robustness testing
- Cyber threats to avionics systems are getting more complex, highlighting the need for clearer guidance on robustness and refutation testing in DO-356A/ED-203A. Right now, there's not enough detail out there for compliance.
- Seeing inconsistent practices because there aren't standard definitions, metrics, or methods for evaluating how effective our cyber testing is. This leads to confusion among suppliers and OEMs.
- Looking to kick things off with a phased plan. First up, engage stakeholders and find a standards body to lead the charge. Then, analyze current testing methods and work towards creating unified metrics and reference test approaches.
- Daniel emphasized the need for alignment with existing work done by SC-216.
- Siobvan mentioned that the expertise present in the community should dictate which industry forum manages the new standards.
- Lilian stated the need for a verification function, suggesting it should be encompassed within ARP 4754, which will be updated to include security considerations.
- Stefan suggested considering other forums besides EUROCAE, RTCA, or ARINC for discussions.
- Stefan summarized that the standards should not outline testing steps but focus on measuring the thoroughness, depth, and breadth of testing related to security.
- Stefan noted that a standard for assessing the quality of testing would enhance trust in security measures.
- Matthieu inquired about the usefulness of existing standards like the Common Criteria in the discussions.
- Nikita stressed the significance of assurance process elements in building confidence, complementing technical Minimum Operational Performance Standards (MOPS).
- Marshall pointed out that MOPS have traditionally been used for Technical Standard Orders (TSOs), indicating specific implementations.
- Nicolas noted that EASA employs NIST 800-115 in their guidelines.
- Lilian suggested developing a refutation standard to cover Ground Support Equipment (GSE).
- Stefan reiterated that existing standards should be leveraged to understand attack surfaces and ensure comprehensive coverage of security requirements.
- Stefan cautioned that developing robust standards and measures will involve significant costs.
- Varun supported a piecemeal approach, emphasizing differentiation for GSE and bridging equipment interacting with the aircraft.
- Daniel was tasked with identifying where the expertise exists to advance these

discussions will work with Siobvan to make the formal recommendation for such a standard (and which organization to own it) via the Aviation Cybersecurity ARC

Next topic- Cyber regulatory compliance

- Anup presented charts on a security certification concern. This is for awareness and may be added to the parking lot items.
- There is an ongoing issue with obsolescence in aerospace, necessitating continuous enhancements in safety and situational awareness.
- Recent updates including FAA NPRM regulations for Aircraft System Information Security/Protection (ASISP) and revised AC/AMCs are calling for new risk assessments and change impact analysis for legacy products.
- Legacy product updates may conflict with new objectives, especially concerning obsolescence, service-related difficulties, and safety enhancements;
- A comprehensive approach is needed to assess risks while maintaining safety and airworthiness.
- Recommendation to focus risk assessments on new functionalities while ensuring they do not degrade the overall safety and airworthiness of aircraft.
- The idea of non-OEM SEC programs was introduced, highlighting a need for flexibility within fleets to avoid downtime.
- Request made to include obsolescence and fleet flexibility issues in the list of parking lot items for further discussion.
- Aneesh expressed interest in having his organization participate in discussions on a testing standard, pending management approval. He also mentioned a pending ARC discussion.
- Stefan emphasized the importance of not exacerbating cybersecurity problems during risk assessments for legacy equipment.
- Nicolas advised to initially conduct a CIA analysis followed by a risk assessment and to consult with authorities on applicable security measures.
- End of Plenary