RTCA Paper No. 027-25/SC216-158
EUR 080-25 / WG72-184

St. Denis and Washington DC, 12/13/2024

EUROCAE WG-72 Meeting #77 / RTCA SC-216 Meeting #68 Joint Plenary **"Aeronautical Systems Security"**	
Date	***Monday – Friday 09-13 December 2024*** ***09:00 – 17:00 EDT / 15:00 – 23:00 CEST*** *Friday 13th ends at 13:00 EDT*
Place	***Embry-Riddle Aeronautical University, Dayton Beach, FL Campus (and Virtual)***
Venue	***Embry-Riddle Aeronautical University (ERAU)*** ***New Resident Hall 1, Room 148 – Building 155*** ***1 Aerospace Boulevard*** ***Daytona Beach, FL***
Hosted by	***ERAU and RTCA***

Attendance:

Contact	Organization	09-Dec	10-Dec	11-Dec	12-Dec	13-Dec
Aaron Renshaw	American Airlines					
Abinash Aryal	Southwest Airlines					
Adam Patrick	Rolls Royce	X	X	X	X	X
Adrian Waller	Thales Group					
Alain Combes	Airbus	X	X	X	X	X
Alan Teyssier	FAA					
Alessandro Oteri	Leonardo	X	X	X	X	X
AmyClaire Brusch	ACI/NA					
Ana Pasuca	IATA			X		
Ana Santos	Embraer				X	
Andrea Cascio	Leonardo	X	X	X	X	X
Andreas Henke	DLH					
Andrew Drake	NetJets					
Andrew Kornecki	ERAU	X	X	X	X	X
Aneesh Sankruth	Gulfstream					
Angeliki Karakoliou	EASA					
Anna Guegan	EUROCAE	X	X	X		X

Anup Raje	Honeywell	X	X	X	X	X
Arthur Pang	Boeing					
Barbara Clark	FAA					
Ben Nagel	CyberBen	X	X	X	X	X
Bernard Margelin	Airbus	X			X	
Bill (William) Trussell	IFR Development					
Billy Ogunsola	UK CAA	X		X		X
Brian Petre	GE Aerospace		X	X		X
Britney Boler	Southwest Airlines		X			
Cameron Wright	Southwest Airlines			X		
Carl Schuett	Southwest Airlines					
Cecil Deleon	Southwest Airlines					
Charles Sheehe	NASA	X		X	X	X
Chris Gorton	UK CAA		X		X	X
Chris Kendrick	FAA-AFS	X	X	X	X	
Chris MacMullin	CA Dept of National Defense					
Christopher Terrington	Collins Aerospace					
Claudio H	Lilium	X	X	X	X	X
Cristian Bertoldi	Airbus					
Cyrille Rosay	EASA	X	X	X	X	X
Dan Diessner	ERAU					
Daniel Salter	UK CAA	X		X		X
David Chen	FAA					
David Harvie	ERAU	X	X	X	X	X
David Pierce	GE Aerospace					
Davide Martini	EASA	X		X		X
Deepak Kamath	FAA					
Emerson Luiz Cunha	EMBRAER	X		X	X	X
Esha Vasdev	CA Dept of National Defense					
Fabian Cavenne	Thales Group	X	X	X	X	X
Felix Meier-Hedde	Airbus	X	X	X	X	X
Filippo Tomasello	EuroUSC Italia					
Florin Grafu	Romanian Air Traffic Services	X				
Francois Triboulet	EASA					
Frédéric Heurtaux	Safran Group					X
Gabriel Elkin	MIT-LL				X	
Garcia-Blanco Castro Borja	EASA					
Garv Stephenson	Wisk					
George Chang	Boeing	X				
Gilles Thales Descargues	Thales Group				X	X
Hagop Kazarian	Bombardier	X	X	X		X
Hannes Alparslan	EDA					
Ian Coaker	BAE				X	
Igor Hoffman	UAL					

Isaac Lee	Southwest Airlines					
Isaac Rodriguez	Wisk					
Isidore Venetos	FAA	X				
Ivan Padilla Muro	UPM Madrid					
J.P. DeKruiff	IOActive Cybersecurity					
Jakub Cunat	Egis Group	X		X	X	X
Jason Schoenbeck	Collins Aerospace		X			
Javier Diana	EUROCAE					
Jean-Paul Moreaux	EASA					
Jeff Burkey	FAA					
Jens Hennig	GAMA					
Jeroen Tuijp	Netherlands Aerospace Center	X	X	X	X	
Joe Reisinger	Astronautics	X	X	X	X	
Johannes Goebel	EASA					
Johannes Kramer	Lufthansa			X	X	
Johannes vanHoudt	FAA	X				X
John Craig - Shift5	Shift5					
John Flores	FAA		X			
John Peace	FAA	X				
Jonathan Lee (MIT LL)	MIT LL					
Jose M. Fernandez	Polytechnique					
Judicael Gros-Desirs	Airbus	X	X	X		X
Kanwal Reen	Collins Aerospace	X	X	X	X	X
Karan Hofmann	RTCA					
Ken Alexander	FAA					
Ken Kitamura	JCAB	X	X	X	X	X
Ken Natividad	Southwest Airlines					
Kevin Harnett	IOActive Cybersecurity					
Kevin Meier	Textron	X	X	X	X	X
Kristof Lamont	Euro Control					
Laurent Leonardon	Collins Aerospace					X
Lawrence Baker	NCC	X	X			
Lee Howard	Honeywell	X	X	X	X	X
Lindsay Rabinko	Triumph Group	X	X		X	X
Logan Cummings	GE Aerospace	X		X	X	X
Lucas Garcia	Embraer	X			X	
Ludovic Donnadieu	Airbus	X				
Luigi Marotta	Crisalion	X				
Luis Lozano	Ineco					
Manon Gaudet	IATA	X				
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	X		X	X	X
Mariusz Pyzynski	IATA					
Mark Bucko	Boeing					
Mark Hingsbergen	GE Aerospace					
Mark Kelley	Belcan	X	X	X	X	X
Marshall Gladding	Boeing	X	X	X	X	X
Martin Call	Boeing				X	
Marty Reynolds	A4A					
Matthieu Willm	Dassault Aviation	X	X	X	X	X
Michael Vanguardia	Boeing	X				
Michael W Davis	FAA					
Michael Welch	FAA					
Mickael Sabelle	Collins Aerospace					
Mikaëla Ngamboé	Polytechnique Montreal					
Mike Goodfellow	ICAO	X	X	X		X
Mike McCartney	FAA	X	X	X	X	X
Mike Noorman	GE Aerospace					
Mike Shalvey	Southwest Airlines					
Mike Tumminelli	Gulfstream	X	X	X	X	X
Mila Obradovic	CA Dept of National Defense	X	X	X	X	
Milton Santos	EMBRAER					
Minh Trang	Airbus	X			X	
Mitch Trope	Garmin	X	X	X	X	X
Nha Nguyen	Boeing		X	X		
Nicolas Durandeau	EASA	X	X	X	X	X
Nikita Johnson	Rolls Royce	X	X	X	X	X
Niv Siva	UK CAA	X	X	X	X	X
Olivia Stella	Southwest Airlines	X	X	X	X	X
Pamela Davis	Southwest Airlines					
Patrick Morrissey	Collins Aerospace	X	X	X	X	X
Peter McNeely	Astronautics	X	X	X	X	X
Peter Tsagaris	TCCA					
Phil Watson	Panasonic					
Phil Windust	FAA	X	X	X	X	
Philippe Dejean	Safran Group					X
Pieter Wessel	CA Dept of National Defense			X		
Prachi Shekhar	EGIS Group					
Raphael Blaize	Thales Group					
Rebecca Morrison	RTCA	X	X	X	X	X
Renuka Chitikesi	Honeywell		X			
Richard Nguyen	Boeing				X	
Rob Segers	FAA	X	X	X	X	X
Roland Olivier	Boeing					
Romuald Salgues	Airbus Helicopter					

Rosemberg Andre da Silva	ANAC-Brazil	X			X	
Sam Masri	Honeywell	X	X	X	X	X
Sanjiv Pimple	Panasonic	X	X	X	X	X
Sarah Stern	Boeing					
Seth Stewart	Pratt & Whitney Canada					
Shane Chen	Aviage Systems					X
Siobvan Nyikos	Boeing	X	X	X	X	X
Sparpano Daniele	Leonardo	X	X	X		X
Stefan Schwindt	GE Aerospace	X	X	X	X	X
Stephen Van Trees	FAA					
Tara Knight	Southwest Airlines					
Ted Kalthoff	Archer Aviation	X	X	X	X	X
Ted Patmore	Delta	X	X	X	X	X
Theresa Adams	Pratt & Whitney	X				
Thomas Parmer	FAA	X	X	X	X	X
Thuan T Nguyen	FAA	X	X	X	X	X
Tim Stelkens-Kobsch	DLR					
Timo Warns	Airbus					
Valerio Senni	Collins Aerospace					
Varun Khanna	FAA	X	X	X	X	X
Vic Patel	FAA					

Day 1 Monday 12-09-2024

SC-216 & WG 72 Plenary Part 1

- Dan Diessner welcomed the group to ERAU and provided facility safety instructions
- Patrick M. and Siobvan N. opened the meeting and greeted participants
- Siobvan and Patrick presented the agenda and facilitated introductions of participants around the room and online.
- Cyrill presented three individuals that have expressed interest in chairing the WG-72. They are Alain Combes from Airbus, Nikita Johnson Needle from Rolls Royce, and Jerry Hancock from Viasat. Alain and Nikita were present. Both Alain and Nikita presented a blurb about themselves. Alain and Nikita were assigned as the co-chairs of WG-72. Everyone congratulated the newly assigned co-chairs.
- Cyrill presented a summary of the responsibilities of the co-Chairs that included overseeing the execution of the work program and Technical Standards in accordance with the Terms of Reference (ToR) and representing the Working Group in Technical Advisory Committee meetings when needed. The co-chairs are also responsible for facilitating WG meetings and lead discussions, coordination with leadership from partner committees, developing and circulate the agenda and calling notices for WG meetings, and ensuring the minutes of Plenary WG meetings are accurately recorded by an individual or on a rotating basis.
- Rebecca Morrison and Anna Guégan presented the RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, participation and membership policies. Rebecca added an export compliance slide that asked that No ITAR data is to be presented at the meeting.
- Hagop Kazarian asked if referencing RTCA and EUROCAE standards in company

processes provided no published content is reproduced requires RTCA's permission.
- Hagop acknowledged that permission is needed to reproduce or present published content.
- Stefan Schwindt confirmed no permission is needed for internal use (like training), but a license for the standards is required, which Bombardier has as an RTCA member. For public discussions (talks, presentations, papers), permission is necessary. Certification processes (cert plans, etc.) can use the documents without permission for papers submitted to FAA/EASA.
- Rebecca responded that you don't need to ask permission to reference if you are using it for internal use, internal training and docs. Rebecca added that recording of meeting discussions is not allowed.
- Alain inquired about integrating white papers into standards.
- Rebecca clarified that integrating white papers into standards is permissible for company white papers, but public white papers must be referenced when writing standards.
- Discussion on how to effectively identify active contributors versus "lurkers" in document collaboration, committee leaders discussed using secretary meeting minutes.
- Anna presented info on the Eurocae symposium scheduled for 23-24 April 2025 in Madrid, Spain.
- Siobvan reminded the group to keep the MVP in mind when working.
- Cyrille provided a summary of the topics presented at EASA's Part-IS workshop in including Part-IS Overview and Organizational Impact. The workshop highlighted the interconnectedness of Part-IS with other rules across various domains and discussed the expected impact on organizational structures. There are ongoing initiatives that are designed to facilitate the implementation of Part-IS within existing regulatory frameworks. Feedback from early implementers of Part-IS was shared, focusing on their practical experiences, challenges faced, and critical aspects. Additionally, the workshop included examples of risks associated with the interactions between organizations, emphasizing the importance of addressing shared risks in the implementation process.
- Cyrill added that the workshop emphasized that a successful implementation of cybersecurity in aviation requires a multidisciplinary approach with collaboration among various functions within organizations, acknowledging that perfection is not expected at the initial stages; therefore, a gradual and steady implementation using a trial and error mindset is encouraged, supported by available guidance and shared experiences from others in the journey.

Regulatory Update:

- Cyrille provided EASA regulatory update on regulations, EU 2023/203 and 2022/1645, along with associated Acceptable Means of Compliance (AMC) and Guidance Material (GM). EASA is actively engaged in updating its regulations. The associated AMC and GM documents updates is scheduled for Q2 2025. A focused consultation process is set for April 2025.
- Varun Khanna presented FAA regulatory update: Varun stated that the FAA NPRM and associated AC comments are being addressed. He added that the rule will be published before Feb 2026.
- Phil added that the FAA 2024 reauthorization act establishes a new Advisory and Rulemaking Committee (ARC) with scope outlined in Section 395 of the act; the committee's charter will be signed and then work begins. Stakeholders can refer to the ARC committees manual for additional guidelines. The manual can be found by searching for "FAA committees" on the internet.
- On the NPRM Stefan questioned that not all comments are published. Varun will check on that and sked Stefan for more details.
- UK-CAA update was provided by Daniel Salter. There is a big focus on the UK ISMS.

The regulation is moving into drafting phase with legal. It will look different from part IS but has the same objectives. UK-CAA hopes to publish in the spring.
- JCAB: Ken Kitamura provided JCAB update. JCAB is trying to develop an infrastructure guideline for cyber. This guideline will include aviation.
- Austrocontrol (Mario) – will present Part-IS TF updates Wednesday
- No updates from Canada and Brazil.

End of part 1 of this week plenary.

SG-3 ISEM:

- Andrew presented agenda topics. The agenda included a review of the updated draft and new proposals.
- Airbus provided two proposals. One for Section 5.4.2: Focused on specific compliance and operational procedures. The second was for Section 6.4.6: Addressed further responsibilities and requirements.
- Discussion on Airbus Proposal for section 5.4.2:
- The proposal received general agreement but noted the need for minor changes, particularly regarding order. A key suggestion was introduced by Andrew, emphasizing that various methodologies and scoring systems exist for identifying vulnerabilities' criticality. It was suggested that each organization should select a method that aligns with its specific assets while adhering to recognized industry standards. This proposal received support from multiple stakeholders, including Marshall, Siobvan, Olivia, Kanwal, Sanjiv, and Adam Patrick.
- An important point raised was the necessity to expand on the criteria for customization within risk assessment methodologies. Participants recommended including guidance on factors to consider, such as: Availability of assessment tools, Ease of vulnerability exploitation, and Specific placements of vulnerabilities within architecture
- Another critical discussion highlighted the challenges of assigning Common Vulnerability Scoring System (CVSS) scores to vulnerabilities that are not directly related to cyber issues or are process oriented.
- Discussion on Airbus Proposal on Section 6.4.6:
- Airbus articulated its goal to reduce vulnerabilities while still ensuring that all necessary information is made available. However, concerns from EASA were raised regarding the perception that this might lead to a reduction in reporting. The consensus was that this goal should not be the primary objective.
- Alain proposed establishing a mechanism, like a database, to communicate with affected customers without disclosing sensitive data.
- Collins added that suppliers have an obligation to report vulnerabilities and defined the need to clarify that airborne software should not be included in Part-IS. Furthermore, if vulnerabilities are mitigated, suppliers are not required to report them, a sentiment echoed by others who advocated for a distinction between aircraft systems and IT/OT systems.
- Garmin cautioned that providing too much information may result in confidentiality issues, while GE argued that the proposal does not sufficiently address IT/OT needs and lacks adequate standards for proving compliance with requirements.
- Southwest supported Collins' comments, especially concerning Ground Support Equipment (GSE). They noted that, as currently written, a supplier might misinterpret the text and assume they are not obliged to inform others about vulnerabilities.
- There was debate over the inclusion of specific vulnerability reporting requirements in the ISMS document, focusing on the relationship between suppliers and operators and whether Part-IS applies to certified airborne products.
- Honeywell suggested reevaluating the terminology from "vulnerabilities" to "risk," advocating for reporting risks instead of raw vulnerabilities. The FAA’s Rob Segar

suggested incorporating the term "exposed" to indicate that users must recognize how vulnerabilities affect software use, thus advocating clarity around "unmitigated" and "exposed" vulnerabilities.

- Dassault emphasized the need to specify what applies to certified versus standard IT systems, suggesting that the objective of decreasing reporting should be reevaluated considering existing vulnerability management frameworks.
- The discussion closed with Thales referencing a point in section 6.4.2.1, which mentions that insignificant risk vulnerabilities do not need reporting but should ensure shared information is verified and relevant to actual risks.
- GE proposed a methodology for vulnerability scoring of products, suggesting CVSS as a starting point, while Andrew emphasized that organizations could have various scoring systems to assess vulnerability criticality, suggesting that the chosen method should be tailored to the specific asset and aligned with recognized industry practices.
- Alain from Airbus led a discussion on vulnerability reporting and its connection to ISMS.
- Kanwal pointed out the necessity of clearly defining vulnerability reporting in supplier requirements to avoid confusion, and Varun expressed concerns about unmanaged vulnerabilities.
- Stefan addressed challenges specific to IT/OT environments.
- The GE proposal on vulnerability reporting was presented by Logan and Stefan.
- The GE proposal highlights the following:
    - The industry should develop a tool for consistent risk measurement.
    - Regulatory authorities will set compliance timelines.
    - It recommends starting with the [DO-356A/ED-203A] appendix E guidelines.
    - A logarithmic decay function will be used in assessments.
- Fleet size must be considered, as noted by Rob and Varun.
- Matthieu pointed out differences in exposure levels.
- The proposal questions how to credit physical security.
- Mitch also raised concerns about the applicability of appendix E, given its varied use among companies
- Nikita introduced a playbook aimed at addressing the Part-IS incident requirements, and presented a flow diagram that clarifies inputs and outputs, along with a spreadsheet of questions for deeper consideration. The diagram bridges the gap between safety and security reporting.
- Nikita will simplify the language for the ED-206A appendix.
- Andrew presented a gap analysis spreadsheet that showed existing gaps in compliance relative to industry standards.
- The 1st draft of the ISEM document was posted on the RTCA and Eurocae servers. Andrew walked through the Eurocae site and showed the location of the draft document.
- During the meeting, discussions centered around the schedule and Terms of Reference (TOR).
- Completion of FRAC may not be feasible by December due to outstanding work.
- Patrick and Siobvan reminded the committee that the six-month flexibility for deadlines would soon disappear with the upcoming RTCA policy update, necessitating an adjustment of dates in the TOR.
- Andrew highlighted the urgency of addressing Part-IS deadlines, emphasizing the need for more time to identify gaps in AMC & GM relevant to ISEM.
- The group considered if an April timeline was reasonable.
- Andrew will share his performance objectives gap analysis with the group to guide the committee on necessary actions and timelines.
- Marshall emphasized the importance of developing a Minimum Viable Product (MVP)
- Stefan pointed out that Part-IS is implicitly referenced in TOR, aimed at outlining performance requirements for AMC & GM.
- Alain suggested defining a target date based on TOR objectives
- GE signaled that they would be concerned if a detailed assessment method, like that

presented by Stefan and Logan, was not included.

Day 2 Tuesday 12-10-2024
SG-5 DSEC

- The SG-5 DSEC meeting covered several key topics in its agenda, including a review of meeting run rules, the Terms of Reference (ToR) and Task Sheet, Minimum Viable Product (MVP), discussion points, timelines, draft document review, and next steps.
- Participants were reminded to keep discussions within the ToR's scope, consider remote counterparts, and avoid circular discussions.
- Olivia added that the primary objective was to create a document outlining minimum standards for data generation, storage, and delivery, particularly focusing on sensitive aviation data. The goals set by EASA and the FAA include securing data in the aviation functional chain and preventing reverse engineering that could compromise confidentiality.
- Olivia discussed following the Minimum Viable Product (MVP) goals by providing a framework to guide on applying minimum data security objectives, alongside secondary focuses on creating a use case to demonstrate the practical application of this framework and specifying data security requirements for specific industry scenarios, such as securing airborne software.
- The group discussions confirmed that all use cases will be informative, and there is a consensus on transforming the report into a formal standard based on industry feedback.
- The need for specific security attributes and clarity on the timing within the aviation data lifecycle was emphasized.
- The initial timeline for document development was presented and included a draft review in December 2024, an end to the comments period in January 2025, and a final review in March 2025.
- A revised MVP timeline that calls for a review of the DSEC report in April 2025 and a possible kick-off for DSEC revision in Q2 2027 was presented and approved.
- Next steps outlined include modifying the ToR to transition the DSEC from a standard to a report, preparing for the Eurocae TAC meeting in January 2025, and conducting a review and comment schedule.
- Additionally, the group is working to reach consensus on definitions for data types, the necessity of data classification sections, and the discussion on the aviation data security lifecycle while making it clear that the DSEC will not reference other documents.
- Finally, the action items from the Q3 plenary include developing clear distinctions between normative and informative sections, evaluating the integration of graphics for airborne software data flow, and discussing integrity checks related to cybersecurity.
- Olivia presented the draft DSEC document. Format of the document will be fixed.
- Olivia provided an overview and went over different sections of the DSEC document. She also went over the general format and structure of the document.
- Olivia presented the 1st use case. Field loadable SW delivery. Olivia discussed the “out of scope” section.
- Anup presented few slides on the use case.
- The presentation on the DO-DSEC Database Use Case history outlined the journey of separating airborne software and database use cases, which were initially combined for simplicity.
- However, as the Aviation Data Security Framework evolved, it became clear that specific guidelines in DO-200B/C required these two areas to be addressed independently. Both use cases were part of the Minimum Viable Product (MVP)-1; however, to keep everything on track and meet the deadlines, the decision was made in June 2024 to descoped the database use case.
- Anup reviewed DO-200/ED76 standards concepts building a crucial framework for

aeronautical data processing/movement—from data originators to end users. With concepts like Data Quality Requirements (DQRs) and Data Process Assurance Level (DPAL), we gained a clearer understanding of the necessary data integrity levels, particularly for avionics-certified applications.

- He emphasized procedures for formal data alterations and the qualification of tools used in data processing, ensuring everything runs smoothly and effectively.
- Anup's presentation acknowledged the need for compliance through robust audit processes and prevention measures against intentional data corruption
- Anup proposed inclusion of the DO-DSEC Database use case in MVP-1, along with airborne software.
- Anup proposed deferring stakeholder identification and end user requirements to MVP-2.
- In the discussions following the presentation, several key points emerged regarding the distinction between data protection and the broader context of Cyber Security Controls (CSC). Thuan from the FAA emphasized this difference, a sentiment echoed by Anup. Stefan noted the importance of aligning these discussions within the general framework, considering both MVP-1 and the pathway to MVP-2. Nikita raised the issue of proportionality, with Anup suggesting that the Data Process Assurance Level (DPAL) should adequately address this aspect.
- The conversation shifted to the importance of consistent systems during data transport, with both Stefan and Anup agreeing that a unified approach is necessary. Kanwal proposed modeling the framework section to better categorize data types, acknowledging a need to add security measures during the development phase to prevent tampering before software is signed for shipping, as suggested by Rob. Anup indicated that such concerns could be addressed as part of the certification process.
- Variability in data types was also discussed, as Rob highlighted differences in the treatment of software based on severity, with Nikita supporting this notion for transport but not for other phases.
- Discussions then pivoted toward potential integration of aviation Public Key Infrastructure (PKI) and digital signatures, which Olivia recommended as part of a use case to meet specific objectives.
- The group acknowledged the ongoing implementation of over-the-air software updates for some critical systems.
- Mitch brought attention to the operational context, noting that databases can be installed by pilots during regular flight operations, unlike software changes, which generally fall under maintenance actions.
- Matthieu added that while military and civilian software and database distribution use cases bear similarities, the security levels differ significantly.
- Alessandro highlighted that the definition of airborne software includes databases, prompting Nha Nguyen from Boeing to suggest mentioning database use cases in the upcoming DSEC release.
- Olivia Stella agreed, proposing that they acknowledge databases as part of the future scope. Ted Patmore emphasized that navigation databases should be treated as a separate use case but remain linked to the integrity and authenticity of airborne software distribution.
- There was agreement that while ground support equipment (GSE) software may authenticate airborne software, it should not be included in the airborne software use case. Ted further asserted that a definition for pre-certified software is needed since most airborne software is certified upon receipt.
- Ted suggested the need for distinct use cases for both ground support information software, databases, and other airborne software.
- Rob pointed out confidentiality as a logistics issue, while Stefan emphasized the groundwork laid by the document, suggesting that if the correct tools and framework are established, the implementation of use cases becomes less critical.
- Olivia continued to review the document draft, providing examples of different data types

for clarification.

- Varun Khanna and Anup emphasized the need for the framework to clearly outline how it should be utilized, adding that use cases should support this guidance.
- Kanwal added that the framework should serve groups rather than individual companies, advocating for a comprehensive approach to minimum requirements related to security goals, like confidentiality.
- As the conversation unfolded, minor terminology adjustments were suggested, such as referencing "CIA" as "Security Attributes" in line with agreed standards. Cyrille highlighted the importance of addressing future connectivity risks and stated that the framework should be prioritized over individual use cases.
- Anup reiterated that the framework is designed to assist other working groups while participants discussed the potential inclusion of a comparative table for confidentiality, availability, and integrity risks, which would facilitate an understanding of different protection levels.
- Cyrille also pointed out the differences in Terms of Reference (ToR) between RTCA and EUROCAE, emphasizing a unified framework approach that encompasses more than just data transmitted to aircraft, including future connectivity risks.
- Kanwal questioned whether the requirements for airborne software were being defined, to which Olivia clarified that the framework would remain at a higher level with any future changes documented accordingly.

Day 3 Wednesday 12-11-2024

- Siobvan- Introduces the agenda for the day.
- Mario Lenitz provided an update on the work of the Part-IS Task Force and its impact on DO-410/ED-ISMS. He emphasized that the task force focuses on various aviation domains, including ATM/ANS, drones, and the responsibilities of aviation authorities in ensuring compliance with information security requirements.
- Mario stated that Part-IS Task Force was established in February 2023 to enhance the implementation of Part-IS regulations across Europe.
- Mario Lenitz provided updates on the task force's activities, highlighting its impact on DO-410/ED-ISMS and emphasizing the importance of building cybersecurity competencies within authorities, particularly those that traditionally focused on safety.
- Mario added that the task force operates independently of industry stakeholders, which allows for a regulatory perspective prioritizing authority-specific needs.
- Key goals of the task force's activities include enhancing cybersecurity skills, harmonizing oversight practices for Information Security Management Systems (ISMS), and facilitating coordination among authorities managing organizations across jurisdictions.
- Challenges identified include limited financial resources and the need for improved inter-authority cooperation to streamline oversight processes while addressing overlaps with existing regulations like the NIS Directive.
- The task force key deliverables include an ISO 27001 Add-On Guidance, and Part IS implementation guidelines.
- The Task Force participants include more than 20 competent authorities such as European Commission, EASA and ENISA.
- The Task Force emphasizes strong communication with stakeholders like Eurocontrol and WG-72 to ensure a cohesive implementation of Part-IS standards.
- Mario stressed that establishing an ISMS is essential for compliance in aviation and safety-critical sectors, particularly as smaller organizations express concerns about the complexity and resource demands of ISMS.
- An open-source HTML-based assessment tool has been developed to assist organizations in evaluating their ISMS compliance and maturity. Nevertheless, there are ongoing discussions regarding the role of standards in compliance, with many

stakeholders remaining resistant to the mandatory adoption of external standards, emphasizing that while beneficial, standards like ISO 27001 are generally not obligatory.

- Daniel Salter expressed the UK's interest in the task force's outcomes and raised concerns about the need for clear guidance on risk assessments, especially for smaller organizations.
- Mario responded that the task force opted not to develop a separate methodology for derogations, instead recommending the adaptation of existing methodologies to incorporate information security threats.
- Davide clarified that the task force focuses on harmonizing oversight approaches rather than creating industry standards, with risk assessments being handled by SC-216/WG 72.
- Matthieu and Mario discussed the assessment tool's flexibility in evaluating compliance and maturity, highlighting its potential to support the integration of SMS and ISMS. Andrew inquired about additional operator involvement, and Mario welcomed their participation for valuable insights on derogations and risk assessments.
- Siobvan presented four options for progressing with the ED ISMS document:
    - **Option 1**: Move forward with DO-410 Revision New to provide immediate guidance to organizations, allowing for lessons learned to be incorporated later.
    - **Option 2**: Pause development until lessons learned are available and rely on EASA Part-IS AMC & GM for guidance.
    - **Option 3**: A middle-ground approach where some sections align with EASA Part-IS AMC & GM (noting that these will be revised in 2025), while other sections reference the group's document where specific details are lacking.
    - **Option 4**: Release the work from Option 3 as an Interim Report (ER), which can be reviewed by the Regulatory Advisory Committee (RAC) early next year and feasibly released in Q1, then decommissioned upon the release of DO-410.
- Siobvan stressed the need to address practical implementation timelines and resource constraints to ensure usability of the document for the industry.
- Andrew supported Option 3 as a balanced solution that provides actionable guidance without creating inconsistencies.
- Anup also advocated for Options 3 or 4 to clarify requirements for suppliers and emphasized the urgency of timely guidance to align with an October 2025 deadline.
- Alain C. recommended prioritizing compliance and critical risk-scoping topics, favoring Options 3 or 4, particularly to assist smaller organizations understand Part IS requirements.
- Kanwal preferred Option 4 to allow more time for incorporating lessons learned, given that their compliance insights would not be ready until January.
- Mitch highlighted the necessity of immediate guidance on risk assessment methodologies and the importance of addressing gaps in AMC and GM.
- Nikita strongly supported interim guidance (Options 3 or 4) to facilitate responses to industry needs and streamline interactions with authorities.
- Ben and Mark Kelley echoed support for Option 3 to gather broader industry feedback. Anup clarified the distinction between Options 3 (interim report) and 4 (formalized standard), expressing flexibility as long as the interim guidance offers actionable advice.
- Olivia S. suggested an initial vote to determine preference between Options 3 and 4.
- Mario shared diagrams mapping the current document to industry needs and advocated for a pragmatic approach to filling immediate gaps.
- Siobvan concluded by acknowledging the aggressive timeline for publishing DO-410 under Option 3, estimating a potential release by July 2025, and proposed continuing discussions after lunch to finalize decisions.
- Siobvan conducted a vote on the preferred options for progressing with the ED ISMS document following previous discussions, which indicated a leaning towards Options 3 and 4. She reminded the participants that the document would not be included in the Acceptable Means of Compliance (AMC) at this time.

- We voted for #4 to make ISMS a report (ER),
- **Action:** Change the TOR and task sheet for both DSEC and ISMS to be reports. Remove reference to DO doc numbers.
- Siobvan highlighted the corporate ISMS approach as a priority and requested Stefan to provide insights on the recent plenary discussions on the topic.
- Lee Howard pointed out potential redundancies in the ISMS sections and suggested integrating them for a more streamlined approach.
- Mitch and Mario stressed the necessity of addressing ISMS for smaller organizations, particularly since it is not currently reflected in the AMC and GM.
- Alain then presented the maturity model, which aligns with ISO 260's requirement for continuous improvement. The model categorizes maturity levels and sub-requirements for effective ISMS management.
- Rob and Kanwal agreed on the importance of refining existing guidance before relying too heavily on the maturity tool.
- **Action:** Kanwal volunteered to work on maturity model matrix
- Cyrille expressed the need for an intuitive electronic tool for the maturity matrix and suggested incorporating a table format like SM001.
- Nikita discussed the evolution of the ISMS facilitation group and the involvement of organizations like Airbus and Rolls Royce in addressing implementation challenges. She listed common issues such as governance, ISMS setup, and alignment with Safety Management Systems (SMS).
- Anup brought attention to the need for consistent interpretations of regulations across different authorities and organizations.
- Lee raised concerns about the responsibilities of Design Approval Holders in reporting safety incidents and the importance of clear communication regarding safety-related reporting.
- Stefan emphasized the need to formalize supplier communication and accountability to enhance clarity and collaboration among stakeholders.
- Nikita also addressed the challenges small and medium enterprises face in risk assessments under Part IS, particularly concerning external consultants' understanding of the regulations. She suggested developing resources to guide organizations in effectively engaging with these consultants. Furthermore, she shared insights from organizations such as Rolls Royce and Lufthansa Technik, highlighting their experiences in transitioning ISMS from implementation to operational phases.
- The discussion highlighted the challenges posed by overlapping scrutiny from multiple authorities and emphasized the value of workshops in providing clarity on compliance expectations and fostering collaboration among various stakeholders.

DSEC Discussions

- Jumping to discussions regarding DSEC, Anup initiated the conversation by raising several key points for consideration, including the need to clarify whether the use case is informative or normative, its scope concerning when development begins (before or after certification), and decisions related to the project's schedule.
- Patrick suggested leveraging a report instead of issuing a formal document release. He expressed uncertainty about how the normative guidance would be invoked since it is not part of the aircraft certification process and asked Varun for clarification. Varun explained that it would be relevant to operational approval and might relate to airline operations, emphasizing that the objective is to raise awareness rather than to certify anything.
- Stefan stated that the report should not be classified as an Acceptable Means of Compliance (AMC) since FAA regulations require the use of consensus standards, which their reports do not meet due to the absence of a Federal Regulation Advisory Committee (FRAC) or Oversight Committee (OC) input. He further noted that non-

certified systems under a Design Organization Approval (DOA) are not regulated in the U.S. because the DOA concept is lacking. In conclusion, Patrick remarked that the best classification for the document would be that of an informative report.

- Olivia reviewed necessary updates to the ToR, transitioning the DSEC from a standard to a report. The DSEC group also plans to document points of consensus and finalize chapters of the report, with specific attention given to definitions, data classification, and the phases of the aviation data security life cycle.
- **Action**: DSEC group to determining normative versus informative sections, incorporating feedback on use cases, and creating graphical aids for better understanding of airborne software data flow, which will be discussed further in subsequent meetings.
- **Action:** Change TOR document classification to report, work and release DSEC document as a report, later release as a standard.

Day 4 Thursday 12-12-2024
SG-6 FAQ Document

- Nikita presented SG-6 FAQ document progress status and reviewed the group goal and document current timeline. Nikita indicated her plan to review the document and agree with the group on Change 1. Nikita mentioned that the previously agreed to March 25 publication date will not change. Nikita also emphasized adhering to house rules.
- Nikita reviewed comments and response to comments with participants.
- Several discussions among the participants regarding the assessment of layered defense. Discussions revolved around defining "defense in depth" and the implications of layered defense to mitigate risks.
- Various opinions were expressed regarding the necessary security measures SAL levels for hazardous and catastrophic scenarios
- The meeting also highlighted the integration of safety and cybersecurity efforts, with Ian Coaker presenting updates on an SAE cyber and safety integration document.
- Several members called for further clarification on the relationship between safety and security measures, with particular emphasis on defense in depth in secure designs.
- Various members reiterated the complexities surrounding security measure classifications and their alignment with safety requirements.
- There were discussions about the necessity of providing text for FRAC, with some expressing concern over the tight deadlines.
- Nikita will be sending text proposals for everyone to review and provide input.
- Varun presented a chart about the FAA DAL E systems that have embedded security controls:
- The primary concern is the potential bypass of DAL E system embedded security controls. Because these systems have the least amount of oversight, and in the FAA process little or no oversight. DAL E itself is built to bypass the cert process.
- DAL E systems are heavy on COTS which may not permit inspection of code.
- Monolithic kernels create opportunities for kernel compromise and thus security function bypass
- Security embedded in DAL E is not a preferred or expected common case. It should be an exception and it would need to be disclosed at the very beginning of the CAA engagement by stating very clearly in the certification plan with the clearly defined approach to demonstrate that security controls are well tested and reviewed to ensure they cannot be bypassed.
- Open questions: (1) Security devices with other certification/accreditation: Where does this leave us for security components which have been certified against other standards?

Common criteria, other?

- The intention of the FAA standards group was to have a framework where these kind of systems could be employed into the larger aircraft as a protective barrier.
- Encryption: Encryption functions will need to evolve over time due to how encryption decays. Need a means to rapidly evolve and roll out these elements. In general, industry is better off using COTS for these functions. As there are many COTS and encryption libraries available. But there are few high DAL security libraries out there which has created an expensive acquisition process (handful of providers) and these have very little mileage (usage, time, under test) associated with them. Encryption will also become more foundational over time (trusted and encrypted boot) to ensure system integrity
- Gilles sought clarification regarding the interpretation of Security Assurance Level 1 (SAL1), prompting Varun Khanna to express that they lack visibility into, necessitating the inclusion of certain security controls.
- Varun raised concerns about integrating these controls into DAL E systems, noting that such inclusions may pose challenges for the FAA due to their potential for being bypassed.
- Nicolas highlighted the complexities introduced by integrating Commercial Off-The-Shelf (COTS) systems and suggested separating the discussion of SAL and DAL due to the difficulties in demonstrating security measures.
- Nicolas stated that robust scrutiny would be required for security functions within DAL E systems.
- Stefan added that DAL E systems extend beyond IFE systems and should not be assumed to be primarily COTS.
- Nicolas added that even systems classified as DAL A could embed vulnerabilities, stressing the importance of meeting specific SAL criteria outlined in the standards.
- Stefan emphasized the importance of identifying which parts of operating systems need consideration to prevent bypassing security controls, which applies to systems across all DAL.
- Matthieu highlighted the challenge of promptly correcting vulnerabilities in DAL A systems
- Fabien expressed concern that applying Security Assurance Level 3 (SAL 3) to DAL E systems could lead to contamination issues affecting other systems.
- In response, Stefan clarified that it is unnecessary to apply SAL 3 to the entire OS; rather, the focus should be on tailoring security measures to relevant components.
- Nikita noted that future discussions would involve types of attacks, portable equipment, and insider threats.
- Martin added that effective vulnerability management should be regarded as a lifecycle effort, indicating the need for continuous attention and improvement in security practices.
- A range of discussions focused on vulnerability management processes and the integration of security measures within aviation design assurance.
- Alain C suggested incorporating internal audits as soon as a company process is modeled.
- Fabien emphasized the importance of linking Security Management Plans to vulnerability management and continued airworthiness.
- Nicolas supported the view that the vulnerability management process should be included in the Product Security Assessment and reflected in the PSecAC.
- The discussion transitioned to the reporting requirements and potential regulatory gaps regarding vulnerability management in products.
- Participants expressed the need to define which vulnerabilities must be reported and how the Security Management Plans aligns with product policies.
- Matthieu added that defining assurance levels for organizational security measures—rather than just technical controls—would be beneficial.
- Suggestions were made to refine the scope of inquiries to differentiate between technical

and non-technical security measures, with consensus that a focused approach is essential for effective risk assessments.

- Stefan emphasized the importance of considering both technical and non-technical aspects of security in aviation systems. He added that relying solely on technical solutions is insufficient, as even the most secure equipment can fail due to human error or misuse. He identified "human involvement" as a critical non-technical factor that must be addressed, suggesting that effective instructions and guidance should be provided to ensure human adherence to security measures. Stefan stressed that manufacturers bear the responsibility to offer clear directions to operators, with the understanding that the effectiveness of these security measures can vary. Ultimately, it is the operator's responsibility to assess and measure the effectiveness of the implemented security operational measures.
- Discussions focused on the relationship between technical and non-technical controls in aviation systems.
- Ben noted the importance of trust assumptions and the validation thereof, advocating for the inclusion of activities that define necessary security controls outside the aircraft's perimeter, emphasizing their relevance in risk assessment, rather than the Security Assurance Level (SAL) considerations.
- Nicolas pointed out the ambiguity in defining operational, managerial, and technical measures within existing regulations.
- Stefan Schwindt highlighted the role of human factors, stressing that effective instructions and operational guidelines are crucial for compliance.
- The group discussed the challenges posed by insider threats and emphasized the need for a balance between organizational and technical approaches
- Matthieu noted that sometimes it's easier and more cost-effective to implement traditional security measures versus expensive technological solutions.
- Martin Call and others discussed trust-related issues concerning passenger devices and the implications of connectivity, and the challenges of treating passengers as trusted entities.
- The need for logging and monitoring functions was debated, with participants questioning whether security levels should apply to such functions, given that they contribute significantly to anomaly detection in security measures.
- Participants discussed the implications of GPS signal accuracy and the potential risks associated with GPS spoofing in aviation safety assessments.
- Stefan added that safety assessments currently do not consider GPS signals to be completely unreliable, suggesting such errors are extremely rare.
- Matthieu pointed out that the likelihood of spoofing incidents in some areas might be as high as one.
- Stefan noted that in the case of a wrong GPS signal being assessed during safety evaluations, it could potentially lead to grounding the aircraft.
- Mike Tumminelli advocated for improving aircraft resiliency instead of trying to "fix" the problem
- Cyrille Rosay contributed that instead of grounding, aircraft should avoid flying into areas where GPS navigation isn't reliable, indicating that safety directives could mitigate the risks.
- Rob added that spoofing is categorized as a cyber issue.
- Patrick emphasized the importance of managing risks posed by potentially faulty GPS signals, suggesting the need to trace how systems consuming GPS data understand and mitigate impacts.
- Mike Tumminelli added that the issue could also be seen as data poisoning.
- Stefan suggested that existing aircraft architectures could incorporate mitigations without changing satellite systems.
- Cyrille emphasized that the reaction of avionics architectures varies, indicating that the architecture's design is critical for determining how systems respond to security

challenges.
- Fabien said that the conclusions drawn from Aircraft Security Risk Assessments should influence architectural decisions, particularly for new aircraft designs.
- It was discussed that there are no legal issues in using HiClass paper on this topic, just an issue of workload.
- **Action:** Honeywell (Anup) volunteered to convert that concept presentation and paper to FAQ since this scope was getting descoped.
- Anup clarified that the topic of hardware diversity vs software diversity CANNOT be covered as there are no updates to the paper.
- **Action:** Thales will contribute to the paper.
- Regarding IUEI section of FAQ: GNSS is no longer trusted. Probability of exploitation is 1 and threat is high. – comments about NPRM already brings this in context.
- Mathieu says, cannot be protected. We can only protect ourselves as consumers of GPS, not fix the issue of spoofing GPS. EASA says – high and probability 1, so they will expect safeguarding. Not expected to handle JAMMING (that is on the country). SPOOFING (yes expected to be handled)
- Patrick and Stefan – contribute to the intent.
- Cyrille – says special committee is setup to address but something needs to be done at the aircraft level.
- Anup – this will be an expectation when NPRM goes live. FAQ should provide guidance on system level protections not necessarily talk about how the problem can be fixed in first place.
- Patrick – proposal for how design assurance for protection function and SAL assurance for its security assurance based FAQ guidance.

Day 5 Friday 12-13-24

WG 72 and SC-216 Plenary Part 2

- Opening remarks by Patrick and Siobvan.
- Siobvan reminded participants that the plenary RTCA and EUROCAE rules and regulations apply for today's plenary.
- Rebecca reviewed RTCA policy, preference to only plan out two meetings at a time
- Can't have conflicts with PMC
- The group expressed issues with not being able to plan a year and more ahead. Testing of conf rooms should happen before plans are made, per RTCA.
- Anup brought up visa concerns
- Meeting minutes for the October 2024 plenary meeting were approved.
- Next meeting dates and places for year 2024 and year 2025 were presented and updated as follows:
  - Next plenary - March 31 - April 4: EASA HQ, Cologne, Germany. A larger room will be available with no limits on attendance.
  - PMC Meeting: March 13, 2025
  - Plenary after will be June 9 - 13: @ Boeing, Seattle, WA. Justification for location accepted, and sound check completed.
  - PMC Meeting: June 26, 2025
  - September 22 - 26: Plenary will be at Austro Control, Vienna, Austria (Original Dates). Justification for location accepted. New Proposed Dates: September 15 - 19, 2025 (Room changes needed for Tuesday and Wednesday).
  - The Summit is scheduled for the week of October 13, 2025, making these dates feasible. Estimated attendance is 25-30 participants, with a maximum historical attendance of 40.
    Sound check required.

- December 8 - 12: Options being considered
- PMC Meeting: December 16, 2025 - No issues reported.
- Potential Locations: Panasonic in Irvine, CA; Southwest in Dallas; RTCA in Washington, DC. Justifications needed for Panasonic and Southwest.
- Next PMC Meetings to Avoid:
    - March 13, 2025
    - June 26, 2025
    - September 26, 2025
    - December 16, 2025

- 2026 Planning: March/April 2026 meeting to be held at EUROCAE, as it has been a couple of years since the last meeting there.

Subgroup status:

SG-3 ISEM Status:

- Andrew presented SG-3 status and progress made thus far including defining what is needed to move forward.
- The group reviewed slides from Alain.
- Reviewed CSDS content. had 3 proposals. 2 from airbus and one from GE.
- Got feedback and trying to rework into proposals.
- The group will flush out content and figure out what is informative and normative, Had a proposal on SIEM.
- Also discussed the timeline, going forward plan with a realistic timeframe, still missing some of the objectives, did a gap analysis, additional proposals are working thru that, need to update the appendix to look at asset classification etc, still discussions on what is needed before FRAC,
- Alain added that the risk items need to be worked.
- Reviewed schedule, may drive TOR changed based on 6 month “wiggle room” going away. TOR markup reflect this
- The group highlighted agreements on proposals, especially regarding the merging of CSDS content into a single appendix. Feedback suggests the need for clearer guidelines in reporting and managing vulnerabilities, particularly distinguishing IT from certified products to avoid overlaps. A timeline is set for the completion of ongoing tasks, including gap analysis and updates on scoring methodologies, with a final goal of publishing revised documents by the end of 2025. .

SG-4 ISMS Status:

- Stefan and Siobvan presented the SG-4 subgroup status and progress made thus far. The subgroup had multiple presentations and discussions:.
    - Mario provided a presentation on the Part-IS task force, clarifying that SG4 comprises only a subset of the impacted stakeholders. He presented an open-source tool for self-assessment that could aid stakeholders in their evaluations.
    - Siobvan led a discussion on the choices for the path forward regarding the ISMS document, where the group collectively agreed to proceed with option #4. Current work would be released as an Engineering Report rather than an initial release of DO/ED-ISMS, with expectations for the report to pass through the RAC process early next year, allowing for an earlier release.
    - Sections of the document needing further maturation were identified, emphasizing the need for objectives to be clearly articulated in both the

main body and appendix.
    - Alain introduced the Maturity Model, garnering general support but acknowledging that some group members required more time to digest it; Kanwal volunteered to work further on this aspect.
    - Nikita presented feedback from the ISMS facilitation group, where key concerns were raised regarding risk assessment, alignment with ICAO, and interpretations relevant to the ISMS.
    - The rest of the meeting was dedicated to reviewing proposed updates to the Terms of Reference (TOR) and the ISMS document structure to achieve consensus on the Minimum Viable Product (MVP), given the new strategy of releasing it as a report.

- **Action** Items:

    - Update the TOR for ISMS and DSEC.
    - Review and approve updated TOR during the closing plenary on Friday.
    - Send updated documents to Anna and Rebecca.
    - Schedule bi-weekly ISMS meetings.
    - Begin document edits based on group feedback.

<u>SG-5 DSEC Status:</u>

- The DSEC has transitioned from a Standard to a Report.
- The end users primarily include standard-making organizations and industry organizations responsible for securing aviation data throughout its lifecycle.
- Primary Goal: To develop a framework offering guidance on how standards-making organizations can implement minimum data security objectives (informative).
- Secondary Goal: To create a use case that provides a practical example of applying the framework (informative).
- The new document will be generated for publication, addressing minimum standards for the generation, storage, and delivery of data, covering areas such as Operational Flight Programs, sensitive maintenance data records, and other security-relevant information. The document will be clear on its Normative vs. Informative aspects
- The timeline for the use case initiation will begin following the certification of the airborne software.
- New Report Timeline – April 2025: Review and Approval of DSEC Report at the Q1 2025 Plenary.
- Q2 2027: Kick-off for DSEC Revision, contingent upon approval.
- **Action:** A request will be made for a DSEC review in 24 months to be included in the ToR.
- **Action:** Update the ToR to reflect the DSEC's change from a Standard to a Report.
- **Action:** Eurocae Technical Advisory Committee (TAC) meeting scheduled for January 14, 2025; to include an updated ToR.
- **Action:** Schedule a Review and Comment (RAC) session, including a vote on the completion of the review and comment process.
- RTCA PMC timeline is to be determined.
- New TOR format, Rebecca will help with that
- Rebecca said that reports can go through RAC or FRAC, we prefer RAC
- Report won’t be decommissioned if we go with standard later, we can refer to it as historical artifact
- Anna’s advice is to replace standard with report until we are ready for report

- Looks like document numbers 409 and 410 are not official yet
- **Action –** Take 409 and 410 out of Brussels meeting minutes before approval, in general scrub notes and presentations of these references

SG-6 FAQ Status:

- Nikita provided updates on the progress of developing the FAQ document, highlighting that content is now available for all sections.
- Meetings included a robust discussion among participants, which led to actionable follow-on engagement with key stakeholders including Thales, Honeywell, and Collins.
- The group emphasized that they are in the "Final Mile" of completion, where feedback gathered from votes and the last plenary session has determined the status priority model for Issues.
- The FAQ Tracker was introduced with a planned timeline indicating that SG6 meetings are set to restart in early 2025, followed by a new planned RAC session in February 2025. The draft of Change 1 is also expected for review in February 2025, with current focus areas being the drafting intent of SAL 1 and the table update.
- It was noted that the informative vs normative distinction is a leading topic.

Coordination with other industry groups:

- SAE Cyber-related Standards (Siobvan, Stefan): Ballot involving Document Number AIR4757, closed on November 19, 2024. The SAE S-18 Aircraft and System Development and Safety Assessment Committee is set to review the "first complete" AIR8480 draft by December 16. An in-person meeting is scheduled for January 27-30, 2025, in San Diego, California, to facilitate further discussions on these topics.
- RTCA SC-223 and WG-108 - DO-379A and ED-262A documents have received approval for publication by the RTCA PMC and EUROCAE TAC. Currently, these committees are in an Active Monitoring phase as they wait for the completion of FAA flight trials and European initiatives (SESAR and IRIS). Post-validation efforts will focus on revising DO-379A and DO-404 to ensure these standards remain relevant and effective.
- ATA Spec 42 Update: The ATA Spec 42 meeting held from November 12 to 14 discussed necessary 2025 updates, including the integration of PKI. Strategies for collaboration with industry groups and the FAA and EASA were also reviewed. The next meeting is on January 29, 2025.
- WG-112/ED-305 Status (Anup): EUROCAE WG-112 is developing ED-305 for eVTOL. The goal is to adapt existing ED 203 guidance for specific eVTOL conditions. Proposals for addressing concerns about COTS components are pending review in the next draft.
- AI/ML Workshop Insights (Stefan, Anup): The RTCA AI/ML Workshop on November 13 covered software development guidelines, safety concerns, and verification processes. The next meeting for SAE G-34 and EUROCAE WG-114 is set for December 2-5, 2024, in Getafe, Spain.
- ICAO Cyber-related Standards Update (Stefan): The ICAO Cybersecurity Panel is working on a draft of the Global Cyber Risk Considerations document. Recent meetings have focused on aviation information security standards and risk assessment criteria.
- A4A Status Update (Olivia): A4A's next face-to-face session is scheduled for January 28-30, 2025, in Dallas, Texas. They are also preparing a D301 Position Paper, aiming for an early 2025 release, as US operators approach D301 certification renewals.
- ARINC NIS Update (Siobvan, Stefan): The ARINC committee held a meeting in September 2024 and is revising several standards, including ARINC 811. The next

meeting is scheduled for January 14-16, 2025.

- ASTM WK82426 Status (Mitch): ASTM WK82426 is updating standards based on regulatory feedback, focusing on Parts 23 Level I-III aircraft. The updates aim to be finalized in the first half of 2025, with meetings planned to address EASA ballot comments and clarify evaluation needs.
- US ACCESS WG Status (Siobvan, Phil): The US ACCESS WG has resumed with Phil Windust as co-chair and aims to engage more proactively with standards organizations. Upcoming meetings are planned for January and March, addressing European approaches for supply chain certification.
- A-ISAC Update (Andrew, Olivia): A-ISAC is organizing several regional AvTech events for 2024 and 2025, including the Americas Regional AvTech in San Antonio on December 3-4, 2024, and subsequent events in Auckland and Washington DC in early 2025.
- ARINC Update (Ted):
    - ARINC is revising ARINC 645-2 for secure software data loading, targeting submission of Supplement 2 for acceptance in May 2025. ARINC 649 and ARINC 827-2 are also being developed.
    - Updates for ARINC 835-2 include a new security process for loadable software parts. This is set for submission in May 2025. Additionally, ARINC 851 is also being worked..
    - The next face-to-face meeting on software distribution standards is scheduled for January 21-23, 2025, in Dallas, TX, to discuss critical updates and revisions in secure software management..
- ECSCG: Cyrille presented key updates regarding Cybersecurity and New ATM Master Plan 2025 that was adopted in December 2024. This plan underscores the importance of cybersecurity within the air traffic management (ATM) framework, outlining a roadmap that defines priority capabilities necessary to bolster the cybersecurity of ATM systems. By 2030, the European aviation ecosystem is planning for cyber resiliency to ensure continuous delivery of operations even under attack. Looking ahead to 2035, the ecosystem aims to evolve from resilience to a state of anti-fragility, where it can learn from cyber incidents and enhance its defenses against new threats. Moreover, the session highlighted the need for coordination between SESAR solutions and the ECSCG, with attention to the EU Cyber Resilience Act, which sets forth compliance obligations for manufacturers and importers, effective December 2024. Upcoming ECSCG meetings are scheduled for February 20 and July 8 in 2025. .
- Agenda for the next plenary meeting will be out soon.

End of day 5.