



RTCA Paper No. 066-25/SC216-159  
EUR 218-25 / WG72-185

St. Denis and Washington DC, 04/04/2025

<b>EUROCAE WG-72 Meeting #78 / RTCA SC-216 Meeting #69 Joint Plenary</b> <b>“Aeronautical Systems Security”</b>	
<b>Date</b>	<b>Monday 31 March – Friday 4 April</b> <b>09h00 – 17h00 CEST / 3h00 – 11h00 EDT</b> <i>Friday Plenary 09h00 – 13h00 CEST / 3h00 – 7h00 EDT</i>
<b>Place</b>	<b>EASA (and Virtual)</b>
<b>Venue</b>	<b>EASA</b> <b>Konrad-Adenauer-Ufer 3, 50668 Koln, Germany</b>
<b>Hosted by</b>	<b>EASA and EUROCAE</b>

**Attendance:**

Contact	Organization	04 April
Aaron Renshaw	American Airlines	
Abinash Aryal	Southwest Airlines	
Adam Patrick	Rolls Royce	X
Adam Smith	SWA	X
Adrian Waller	Thales Group	
Alain Combes	Airbus	X
Alan Teyssier	FAA	
Alessandro Oteri	Leonardo	X
AmyClaire Bruschi	ACI/NA	
Ana Pasuca	IATA	
Ana Santos	Embraer	
Andrea Cascio	Leonardo	X
Andreas Henke	DLH	
Andrew Drake	NetJets	X
Andrew Kornecki	ERAU	
Aneesh Sankruth	Gulfstream	
Angeliki Karakoliou	EASA	X
Anna Guegan	EUROCAE	
Anup Raje	Honeywell	X
Arthur Pang	Boeing	
Barbara Clark	FAA	
Ben Nagel	CyberBen	X
Bernard Margelin	Airbus	X
Bill (William) Trussell	IFR Development	
Billy Ogunsola	UK CAA	X
Brian Petre	GE Aerospace	
Britney Boler	Southwest Airlines	
Cameron Wright	Southwest Airlines	
Carl Schuett	Southwest Airlines	
Cecil Deleon	Southwest Airlines	
Charles Sheehe	NASA	X
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	X
Dan Diessner	ERAU	
Daniel Salter	UK CAA	X
David Chen	FAA	
David Harvie	ERAU	
David Pierce	GE Aerospace	

Daide Martini	EASA	X
Deepak Kamath	FAA	
Emerson Luiz Cunha	EMBRAER	X
Esha Vasdev	CA Dept of National Defense	
Fabian Cavenne	Thales Group	
Felix Meier-Hedde	Airbus	X
Filippo Tomasello	EuroUSC Italia	
Florin Grafu	Romanian Air Traffic Services	
Francois Triboulet	EASA	
Frédéric Heurtaux	Safran Group	
Gabriel Elkin	MIT-LL	
Garcia-Blanco Castro Borja	EASA	X
Garv Stephenson	Wisk	
George Chang	Boeing	
Gilles Thales Descargues	Thales Group	
Gregg Slade	Leonardo	X
Hagop Kazarian	Bombardier	
Hannes Alparslan	EDA	
Ian Coaker	BAE	
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
Jason Schoenbeck	Collins Aerospace	X
Javier Diana	EUROCAE	
Jean-Paul Moreaux	EASA	
Jeff Burkey	FAA	X
Jens Hennig	GAMA	
Jeroen Tuijp	Netherlands Aerospace Center	
Joe Reisinger	Astronautics	
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	X
Kanwal Reen	Collins Aerospace	X
Karan Hofmann	RTCA	

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	X
Lawrence Baker	NCC	
Lee Howard	Honeywell	
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	X
Marcus Labay	FAA	
Marcus Session	ACI/NA	
Marie-Chantal Mouret	Airbus	
Mario Lenitz	Austro Control	X
Mariusz Pyzynski	IATA	
Mark Bucko	Boeing	X
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	
Mickaël 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	X
Milton Santos	EMBRAER	
Minh Trang	Airbus	X
Mitch Trope	Garmin	X
Nha Nguyen	Boeing	

Nicolas Durandau	EASA	
Nikita Johnson	Rolls Royce	X
Niv Siva	UK CAA	
Olivia Stella	Southwest Airlines	X
Pamela Davis	Southwest Airlines	
Prachi Shekhar	EGIS Group	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	X
Rebecca Morrison	RTCA	X
Rebecca Roberts	Collins	X
Renuka Chitikesi	Honeywell	
Richard Nguyen	Boeing	
Rob Segers	FAA	
Roland Olivier	Boeing	
Romuald Salgues	Airbus Helicopter	
Rosemberg Andre da Silva	ANAC-Brazil	X
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	X
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	X
Thuan T Nguyen	FAA	X
Tim Stelkens-Kobsch	DLR	
Timo Warns	Airbus	
Valerio Senni	Collins Aerospace	
Varun Khanna	FAA	X
Viana Tavares	Embraer	
Vic Patel	FAA	

## Day 1 Monday 03-31-2025

### SC-216 & WG 72

- Andrea Bandieri welcomed the group to EASA and provided facility safety information. He emphasized his support for the industry and asked that the group put quality over deadline. He added that there is a need to maintain commitment to a safe environment and to create a resilient system.
- Nicola D added his welcome.
- Siobvan added an opening remark. Looking to get consensus for three reports this week. Looking forward to working with everyone.
- Nikita Johnson and Alain Combes opened the meeting and greeted participants
- Nikita presented the agenda and facilitated introductions of participants around the room and online.
- Rebecca and Anna were introduced and both presented the beginning slides on membership and proprietary info. Etc.
- Working session all week until plenary on Friday.
- Introduction, in the room and online
- Regulatory updates:
  - Davide shared updates to the regulations. He added that there is not going to update regulations in the coming months, He added that a task force had worked on oversight strategy-According to the complexity of the project.
  - Nicolas added that there is an update to CS23 recognizing ASTM guidelines for SAL level 1-3. There will be an update for TSO subpart A, to introduce security similar to the FAQ doc. There will be update on MC2042, part 27 and 29. Update will be in the new ASTM standard.
  - Varun added that the FAA is working on the AC.
  - Rosemberg added that within ANAC they are learning ground rules for putting cyber in the in the regulation as well as for an example to begin with.
- SG-5 Olivia:
  - Olivia presented updated timeline and shared the most recent version of the report. Olivia reviewed various updates. The group acknowledged the report's relevance for regulators.
  - Varun highlighted the importance of having a holistic approach when dealing with issues that cross the boundaries between air systems and ground systems. He argued that it is not feasible to enforce specific standards solely on air systems, emphasizing the need to consider the entire context.
  - Varun discussed the need to clearly communicate industry standards.
  - The discussion further pointed out that the report should reflect a comprehensive view that accommodates diverse stakeholder positions. This would enhance its acceptance as both a guidance document and a potential means of compliance reference for regulatory bodies. Varun and the team agreed on the importance of structuring their discussions to maintain clarity regarding the document's purpose and expected outcomes.
  - Stefan emphasized the collaborative nature of their efforts within the AIA and acknowledged the challenges in coordinating various internal and external parties to ensure timely submissions.

- Stefan mentioned that both the FAA and EASA emphasize the importance of integrating consensus standards into the operational activities. He clarified that the industry cannot independently declare something to be an AMC; this responsibility lies with the authorities who identify and designate AMCs. He mentioned that if we want to propose something as an AMC, we need to specify which rule it is supposed to be an AMC for
- Nikita agreed, stating that no standards or guidance documents should refer directly to what qualifies as AMC. She noted that there are challenges in SG6 related to this issue and suggested that a systematic method is required to bridge the current gap.
- The dialogue pointed out the need for the standards to align with existing aviation safety regulations, asserting that data security should be part of the broader safety framework in aviation, particularly emphasizing the relationship between data security and aviation safety.
- Patrick suggested that system security design requirements should also be added to the discussion.
- Olivia reviewed further updates to the document.
- Cyrille Rosay shared that ED-77B (DO-200C) has entered open consultation that day, though he had not checked for any information security-related changes yet.
- Siobhan mentioned that she coordinated with a co-chair regarding their documents and felt they were aligned.
- Siobhan emphasized the importance of documenting the sources of requirements to improve clarity.
- Logan raised an editorial point regarding the phrasing in the "Secure loading vs. secure distribution" section, recommending the removal of "as defined in ARINC 667" since the scope section already provides relevant definitions.
- Nicolas questioned how security measures would align with the applicable standard chapter.
- Stefan explained that some companies manage their maintenance without using external Part 145 and secure their data loaders within their IT framework.
- Olivia proposed evaluating specifics in section 4.5 to ensure coverage of the topics discussed.
- Nicolas highlighted that ARINC 645-1 might be overly stringent in some cases, while also mentioning that PKI should not be mandatory.
- Stefan pointed out that ARINC standards often cover specific implementations, suggesting a focus on overall objectives within DSEC, such as the required cryptographic strength rather than specific signing methods. He supported standardization but expressed the need for flexibility to accommodate evolving technical implementations.
- Varun agreed with Stefan's perspective.
- Ben updated the group that the most recent standard is FIPS 186-5.
- Andrea pointed out the issue of CRC collisions versus SHA256, depending on the protection needs.
- Andrew suggested using "Acceptable methods" instead of "Recommended methods" and raised questions about the applicability of discussed methods in the future of Advanced Air Mobility (AAM).
- Patrick reiterated the need for cryptographic measures with an acceptable strength, proposing to separate requirements into categories.
- Rob warned against the false security of assuming integrity alone is sufficient in closed systems.
- Stefan emphasized the need to define adequacy for different severity levels throughout the document, while Nicolas advocated for a robust mechanism to ensure integrity.
- Mitch outlined the need for selecting cryptographic and transfer mechanisms that ensure integrity and authenticity of airborne software.
- Nicolas reminded the group of existing requirements for authenticity in airborne software.

- Lastly, Stefan indicated that there needs to be clarity on how "acceptability" is defined in the document to avoid vagueness.

## Day 2 SG-6

04-01-2025

- Nikita presented the agenda for the day.
- Johannes provided a presentation on EASA's perspective on security measures, SAL assignment and defense in depth.
- Johannes presentation emphasized the application of defense in depth for any threat condition. His presentation offered more flexibility in recognizing SAL 1 for non technical security measure such as SAL allocation for ground equipment. He also discussed approaching diversity, independence and isolation depending on threat condition.
- Johannes discussed the integration of risk assessment in relation to product security measures within a certification environment. He emphasizes the importance of acknowledging existing controls in the environment to claim credits during the product risk assessment. He mentioned that procedural and technical controls outside of certified products, particularly within an ISMS, play a crucial role in assessing security measures.
- Additionally, he highlight a distinction between certifying products and claiming credits for measures implemented in the risk assessment as part of a defense-in-depth strategy..
- Philip raised a concern about the contradiction between not certifying ground equipment and assigning it an assurance level (SAL2), questioning the validity of such claims without certification.
- Stefan pointed out the inconsistency in assessing human activities for security controls (operational controls) using Security Assurance Level. The inconsistency is that SAL addresses technical solutions only
- Mitch added that not every operator must adhere to Part-IS regulations.
- Stefan highlighted a significant issue regarding the differing definitions of "unsafe conditions" between the FAA and EASA (European Aviation Safety Agency). He noted that if "Major" is justified as being SAL2+SAL1 in relation to these unsafe conditions, it could lead to a breakdown in regulatory harmonization. The FAA and other agencies have specifically retained the classification of unsafe conditions only for catastrophic (CAT) and hazardous (HAZ) situations, while EASA has broadened the definition to include "frequent" major conditions.
- Stefan emphasized that, under EASA's framework, it is permissible to implement security measures when the highest threat level for an aircraft is classified as Major.
- Mitch added that there are certain Supplemental Type Certificates (STCs) where modifications only affect Major or lower function classifications, implying that not all safety measures will lead to a higher classification.
- Stefan emphasized the need to address root causes rather than symptoms, advocating for a deeper understanding of how to analyze and demonstrate concepts like Diversity, Independence, and Isolation (DII) instead of outright disallowing certain architectures.
- Sarah agreed, noting the connection to defining architecture more clearly.
- Logan expressed concern over the prescriptive nature of the requirements for architecture, suggesting that it might hinder innovative solutions.
- Nikita presented a slide reminding everyone of the purpose of the FAQ document
- Nikita presented an updated version of the FAQ document and reviewed it with the group.
- Rebecca presented a slide on comments and handling review comments for DO and ED

documents publication

- Stefan expressed concern about reaching consensus without a non-concur and Olivia inquired about the tools that were available to address this issue.
- Stefan explained that under U.S. law, the Federal Aviation Administration (FAA) (FAA Order 8000.376 and OMB Circular A-119) could directly use only "consensus standards," and a report did not fulfill this requirement. However, he noted that they were permitted to incorporate material from consensus standards into reports. He added that DO/ED documents were cited as Acceptable Means of Compliance (AMC) because they included industry-wide comments and were recognized as consensus standards.
- Aneesh sought clarification, asking for a refresher on the reasoning behind converting these documents into reports for those who were unable to attend all the meetings.
- The discussion recounted a meeting regarding the ER-ISMS in December 2024, where Siobhan presented four options for progressing with the ED ISMS document. The options were:
  - Option 1 involved moving forward with the ISMS document to provide immediate guidance to organizations, incorporating lessons learned later.
  - Option 2 suggested pausing development until lessons were available, relying on EASA Part-IS AMC & GM for guidance.
  - Option 3 proposed a middle-ground approach where some sections aligned with EASA, while other sections referenced the group's document where specific details were lacking.
  - Option 4 suggested releasing the work from Option 3 as an Interim Report (ER) for review by the Regulatory Advisory Committee (RAC) and possible release in Q1, to be decommissioned upon the release of ISMS .
- The group voted for Option 4.
- Ben mentioned that a similar approach was followed for DSEC.
- Stefan noted they produced a report to limit the scope of comments and had the option to release a FAQ as a full document but chose to release a report instead. For ED203A/DO356A, the group chose to go for a Change 1 to limit scope and have a FAQ to accompany it too
- Matthieu suggested including only non-controversial items in the FAQ to minimize collateral impacts on ongoing projects.
- Rebecca Morrison from RTCA pointed out that ISMS had not been assigned, so the designator should not be used.
- Nikita presented a classification of collected comments and their status
- Stefan pointed out ongoing major updates needed in the current text, while other contributors highlighted terminology misuse and urged adherence to established standards like DO-178 and DO-254. Stefan alongside others critiqued the inclusion of unnecessary "shoulds" and "shall" across documents, underscoring the importance of evolving language standards.
- There was a consensus to avoid pitching alternative DALs not recognized, with Stefan emphasizing that using "Shall" in process documents restricts flexibility. The discussion concluded with suggestions on document revisions and terminology clarifications.

## DAY 3

4/2/2025 SG-3

- Andrew presented the subgroup status and updated document timelines. The update will provide guidance on vulnerability scoring. Andrew reviewed new and updated definitions and objectives, Andrew added that the document will provide timeline guidance that will be an informative suggestion.
- Matthieu suggested aligning criticality to the notion of safety significance in ED-ISMS (safety criticality taking into account distance to aircraft) for ground systems. He added that all this guidance has to be written with appropriate caution to minimize the risk that an authority transform it as mandatory timelines
- Stefan highlighted the need to clarify existing mandatory timelines to prevent misinterpretation, ambiguity or gaps. For other legislation such as GDPR, lack of definition by industry in standards led to courts determining criteria. Should aviation industry fail to determine factor for timelines, it will be ultimately decided in court by lawyers and likely not favorable to the teams who need to implement detection and notification
- Adam Smith from Southwest acknowledged the variability in what triggers compliance despite clear timelines.
- Marshall questioned the industry's acceptance of GDPR's applicability to airplane product security, noting that many organizations were already adhering to it for information security.
- Stefan affirmed that GDPR pertained to any personal information of individuals in the EU and EEA, regardless of the data system used.
- Olivia suggested incorporating "Modifications from DO-355 revision" in the upcoming Rev B.

Back to DSEC DOC Olivia:

- There was a discussion on updating the parking lot items and reviewing document revisions. Siobvan suggested a more detailed discussion about the parking lot items process at the next leadership meeting.
- Olivia went through the DSEC document, addressing comments and responses, making edits as needed.
- Mitch added that security treatments for database delivery resemble those for software delivery and noted that practitioners could adapt the material, accordingly, referencing Chapter 4.
- Ted Patmore differentiated between software and data, emphasizing that both involved digital information, with software containing executable instructions and data primarily being informative. He pointed out that in the context of their discussion, "software" encompassed both software and data, asserting that methods like PKI certificates and digital signatures applied equivalently to both categories. Varun concurred with Ted's insights.
- Siobvan raised a question regarding including references if materials were generated by

- committee members and unpublished, to which Olivia indicated she did not think so.
- Siobvan recommended changing "objectives" to "recommendations" for consistency.
- Olivia continued making editorial adjustments throughout the document review and said that she planned to ask the group for consensus on readiness for RAC. Alessandro also provided an update on modifying a figure to show a double arrow from the aircraft.

Next the group moved to work on the FAQ-356 change 1 document

- Nikita shared the scope that the committee had agreed on:
- Stefan shared that DO254 is undergoing revision right now however, DO254 does not have informative material. He added that DO178 uses appendix and annex as differentiating informative vs. normative without specifying the terms.
- Matthieu emphasized that the high-level objective of Chapter 5 should be defense in depth, which involves having resilience against the loss of one or more security measures. He argued that while terms like "independence" may serve as guidance, they are solutions rather than objectives.
- Hagop raised concerns that many of the directives were not aimed at DAHs and questioned their normative applicability.
- Stefan clarified that the "should" and "should not" statements in Chapter 5 were intended colloquially to assist architects, not for compliance purposes, which is why they were framed informatively.
- Logan mentioned that adding logging objectives to a specific change would alter the means of compliance, potentially complicating the project.
- Bernard highlighted that changes related to logging were designated for Rev B.
- Matthieu noted that the SAL3+SAL1 requirements for HAZ could pose problems for legacy systems, and he warned that making Chapter 5 normative would necessitate a significant rewrite.
- Mitch agreed with Matthieu on these considerations and expressed concern about how to define a sufficient level of defense if "defense in depth" were made normative.
- Stefan reiterated that existing normative sections already cover necessary points, supporting the informative nature of Chapter 5.
- Matthieu noted a shift among authorities towards a stricter interpretation of Acceptable Means of Compliance (AMC), urging attention to the wording. Matthieu questioned why previously acceptable practices were now causing concerns.
- Stefan suggested that other important topics to address in Change 1 include updating the Supplemental Type Certificate (STC) guidance and incorporating material from the FAQ draft that should also belong in Change 1.
- Stefan mentioned that specific requirements such as SAL/DAL should be included in Change 1.
- Siobvan acknowledged that they had divided topics between the FAQ and Change 1, and discussed the differentiation between Change 1 and Rev B.
- Matthieu concluded that items like the SAL allocation table and the distinction between normative and informative content were more appropriate for Rev B discussions due to their controversial nature.
- Further discussions primarily addressed the topics that should be included in the FAQ and Change 1, emphasizing the need to focus on non-controversial items.
- Matthieu argued that only non-controversial topics should be placed in either the FAQ or Change 1.
- Ben suggested updating the FAQ based on a previous discussion regarding physical security, proposing that physical and operational controls should be considered acceptable if supported by evidence of their effectiveness.
- Stefan commented emphasizing the necessity to discuss and make progress on significant topics for Change 1, specifically physical security, SAL/DAL, and STC updates.

- Matthieu expressed that updating the table 4.4 was not feasible without addressing legacy systems and recognizing external security measures.
- Marshall inquired about including a note regarding legacy equipment's special considerations.
- Mitch raised the complexity in defining "legacy," while Stefan pointed out that "legacy" lacks a legal definition, which complicates its application.
- Sarah suggested submitting an Alternate Means of Compliance if legacy equipment couldn't meet new Minimum standards.
- Stefan reiterated the need to finalize contentious issues as part of the multi-year Rev B effort.
- Mark questioned whether Rev B would open the entire document for review, to which Stefan confirmed that it would.
- Matthieu cautioned against errata, stating that it poses risks of retroactive applications to ongoing projects.
- The discussion continued with various technical discussions about documents like DO-178, EUROCAE ED-143, and their relevance to Change 1, highlighting the importance of compliance standards and adaptations in certification processes.
- Stefan pointed out that the FAQ could not be published without clarity on the roadmap for Change 1.
- Siobvan responded with several reasons for wanting to release the FAQ as a report instead of a standard. She expressed surprise that this issue had not been raised earlier, particularly during the previous discussions in June when their Terms of Reference (TOR) were approved.
- Siobvan outlined the following key points:
  - Companies are currently using RTCA and EUROCAE standards and have pressing interpretation questions that must be addressed as they develop certification evidence for regulators.
  - Publishing the FAQ as a report would expedite the dissemination of this information, as reports can undergo review through RAC on a shorter timeline.
  - The intended release does not represent changes to MOC but rather offers clarifications, making a report appropriate.
  - The FAQ will not outline methods, processes, or requirements, serving primarily as a Q&A format.
  - Since there are no requirements included, the FAQ does not need to be normative, allowing for an informative report to be used effectively.

DAY 4:  
SG-4 ISMS  
4/3/2025

- Siobvan facilitated Introduction for the new people on the call and presented document schedule.
- Alain Combes, Matthieu Willm and Nikita Johnson presented a report from ASD ISMS facilitation group and SAB WP#61.
- The group presented part IS requirement to systematically identify interfaces with other entities to assist in risk management
- Mario presented the working group context and scope that included airworthiness, licensing and ATM and explained Part IS implementation challenges.
- Key objectives for the task force is to harmonize the process for applicable organizations. Mario explained how the process will work in a systematic way. Mario pointed to using ISO27001:2022 ISMS as a guidance.
- Ben provided a link to the Guidelines: <https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables> and the link to Oversight Approach: <https://www.easa.europa.eu/community/topics/part-oversight-approach-guidelines>
- Mario presented an available alpha-test assessment tool that was developed by Alexander Eckert-LBA
- Matthieu expressed appreciation for the oversight approach discussed. However, he raised concerns that the new requirements appear to be more stringent than what Civil Aviation Authority expects for compliance.
- Matthieu highlighted discrepancies in the expectations for the Information Security Management System (ISMS) between EASA and other civil aviation authorities. He also raised concerns about the oversight approach, which states that an organization will only be deemed compliant after a successful audit of the "operating" level, potentially occurring long after the compliance deadline. He questioned whether this could pose a legal issue, especially in the event of a serious incident beforehand.
- Daniel Salter contributed to the discussion by updating attendees on the timeline for UK Part IS going to parliament, indicating delays in the draft of the Statutory Instrument due to government priorities but remaining optimistic that it would proceed around Q3 of this year.
- Nikita emphasized that the FAQ represented months of collaboration from various groups, emphasizing that effective risk management is crucial for integrating security with safety, which has been a primary topic of discussion.
- Stefan also mentioned the necessity of obtaining intellectual property (IP) allowance for using a specific diagram.
- Rebecca Morrison from RTCA highlighted the approximate six-week timeline for obtaining reproduction permission from ICAO, noting that it has never been denied and

- stressing the importance of securing it before proceeding to FRAC
- Stefan noted that there is a lack of differentiation between categories such as CAT, HAZ, MAJ, and MIN. He pointed out that while groups consider factors related to detectability, they are not adequately accounting for severity, which is an important factor in determining likelihood. He emphasized the need to consider both technical and process means of protection and their effectiveness when assessing likelihood.
- Siobvan referenced the four different "example methods" included in document 203A, while Stefan added that caution is required in discussing the functional chain, as not all stakeholders have full visibility and oversight of it.
- Matthieu suggested viewing the risk assessment matrix as a 2D projection of a 3D matrix that encompasses consequence, distance to safety effect, and likelihood. He clarified that the definition of security measures is critical, distinguishing between IT security measures aimed at mitigating IT attacks and business process security measures that could prevent the propagation of consequences. With this distinction, he asserted that there should not be any double counting of risks.
- Kanwal presented slides from a Part IS Risk assessment methodology workshop
- Mark Kelley went over remaining comments and suggested resolutions.
- Nikita went through more comments and resolutions.
- Stefan noted that Part IS does not utilize the concept of threat condition; instead, it focuses on information security risk. This approach helps to avoid conflicts with threat conditions relevant to aircraft certification.
- Stefan further elaborated that Part IS guidance material employs terminology such as "threat source," "attack vector," and "threat actor."
- There was a discussion that centered around the distinction between external reporting requirements to authorities regarding incidents and versus risks.
- Matthieu questioned whether external reporting pertains specifically to incidents and not risks.
- Stefan clarified that reporting involves both vulnerabilities and incidents, indicating that such reports imply risks if they fall under those categories. He noted that if incidents do not meet reporting criteria, then no reporting is necessary.
- Matthieu affirmed that this falls under the scope of Information Security Event Management (ISEM) topics.
- Stefan added that monitoring, review, and reporting processes facilitate adjustments in response to new threats.
- Stefan expressed that retaining vulnerabilities in the risk assessment documentation would necessitate updating the assessment for each identified vulnerability.
- Alain suggested that known vulnerabilities and threats could still be included as inputs for assessment and managed through Information Security Event Management (ISEM).
- Stefan also introduced the topic of management of change, underscoring that it is a distinct yet crucial issue.
- Alain referenced ICAO Annex 19, emphasizing the necessity for service providers to develop processes that identify changes affecting safety risks associated with aviation products or services.
- Adam proposed that continuous improvement should be treated as a standalone section.
- Siobvan noted that risk change management is an essential focus area.
- Stefan added that the document applies management of change to changing processes rather than risks already under monitoring.
- Ted reiterated the concept of continuous process improvement being supported by continuous risk monitoring.
- Stefan emphasized the need for consistency in terminology, noting that "consequences" and "impacts" were being used interchangeably. He concluded with a call to include validation in the risk assessment to ensure that the right measures are proposed and verification in the actual risk treatment to confirm those measures are effectively applied.
- Stefan expressed that retaining vulnerabilities in the risk assessment documentation

- would necessitate updating the assessment for each identified vulnerability.
- Alain suggested that known vulnerabilities and threats could still be included as inputs for assessment and managed through Information Security Event Management (ISEM).

DAY 5 Plenary day  
4/30/2025

- Nikita and Alain opened the meeting and greeted participants
- 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.

## **Subgroup status:**

### SG-3 ISEM Status:

- Andrew presented SG-3 status and progress made, timeline, gap analysis, scoring updates and proposed going forward plan.
- The group discussed the options presented and decided to go for the proposed plan to revise document to RevA.
- There was a discussion that revolved around organizing the timeline and objectives for Rev A revision. Siobvan noted that while the separation of IT from OT was important, it did not fall within the scope of Rev A as outlined in the TOR. The group planned to address the handling of the document in the next plenary meeting.
- Olivia Stella raised a point about ensuring that the objectives for "Rev B" were documented for future reference, which was referred to as the "parking lot."
- Stefan Schwindt expressed concern about whether the group could finalize their discussions in the current meeting, suggesting that another follow-up meeting might be necessary. He also emphasized that the publication timeline was unrealistic for July, indicating that they had missed an update that Davide had mentioned.

### SG-4 ISMS Status:

- Siobvan presented the SG-4 status and progress made, timeline. Vast majority of comments were reviewed. The ISMS will be a report. The report need to be ready by May 15<sup>th</sup>. A virtual plenary is planned in May to resolve remaining comments pre-RAC.
- Mark noted that the pre-RAC process had been beneficial and suggested that dropping material that was not mature should help in moving forward with RAC.
- Stefan and Patrick expressed support for this approach.
- Alain reiterated the importance of the report for potential customers who were looking for implementation guidance and stressed the need for a timely release by October.
- Olivia asked if there were examples of reports that presented both sides of an issue.
- Matthieu Willm indicated that controversial material should be removed, noting that it

would be treated in a future version, which led the group to agree to advance the document to RAC. There was a motion to proceed to RAC, which was approved unanimously, with proposals from Thales and comments from several members about the importance of the document's acceptance.

- Stefan also inquired about any thoughts from Flight Standards regarding the use of the ISMS document.
- Varun noted that ISMS would not be required in the U.S. for some time, emphasizing this concern for the airlines.
- Mike McCartney from FAA confirmed that he was not aware of any developments related to that and acknowledged the group's decision to move forward with the ISMS discussion to RAC, promising to communicate the RAC schedule and details.

#### SG-5 DSEC Status:

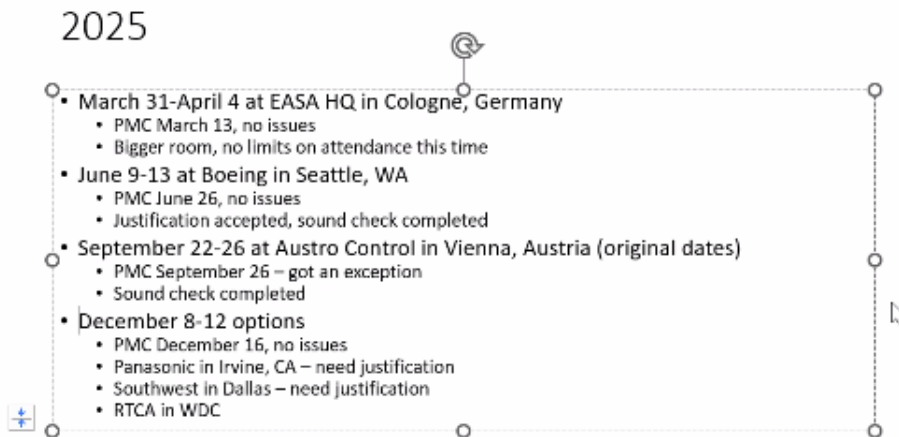
- Olivia presented SG-5 status and progress. The document was voted to go to RAC. There is a planned vote to publish during a possible May virtual plenary. Report is planned to be submitted for publishing on May 16<sup>th</sup>.
- Rebecca agreed with the proposed schedule stating that a plenary is necessary once comments resolution is complete.
- Rebecca mentioned the necessity of implementing formatting across multiple documents by May 22<sup>nd</sup>.
- The group votes in favor of taking the DSEC document to the RAC

#### SG-6 FAQ Status:

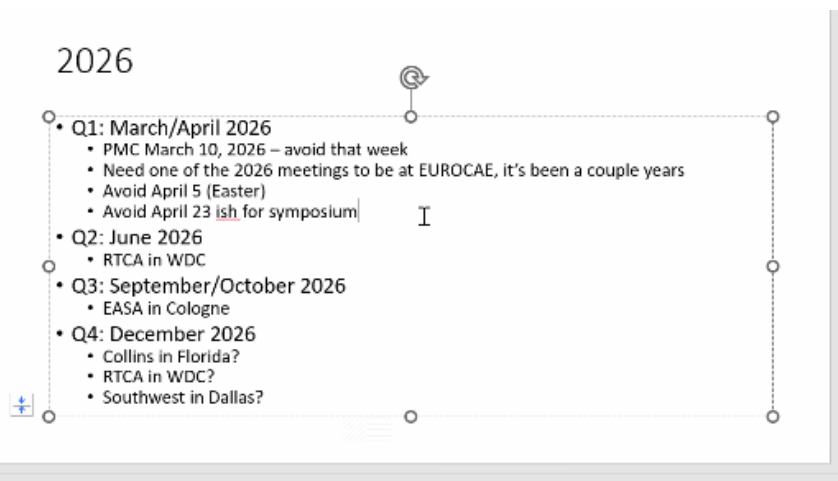
- Nikita presented SG-6 status and progress. She reflected on the maturity of the completed work. Nikita discussed a plan to submit the document for RAC.
- Nikita presented evidence of readiness for RAC reviews
- Nikita presented a new proposal for the FAQ report to go to RAC .
- Nikita presented remaining topics that will be parked for future work
- All comments from RAC will be addressed
- What is being deferred is documented in a file. ER FAQ 1G working is the file that has what is going to RAC. Not all comments have been addressed. The architecture section and the special condition section contain the comments that have not been addressed.
- Nikita discussed the status of the DO-356 Change 1 update.
- Nikita will provide version H by Monday for people to review. This document is planned to be internally reviewed. A decision to go to RAC will be made a week from now.
- Document will not be ready for the June PMC but PMC members can be made aware and they have an opportunity to do an out of cycle review for FAQ.
- Siobhan presented next activities and meeting dates and places for year 2025 and year 2026 were presented and updated as follows:

- RAC Vote on April 4<sup>th</sup> 2025
- Commenting opens on April 7<sup>th</sup> 2025
- Commenting closes on May 6<sup>th</sup> [30 days]
- Comment resolution starts on May 7<sup>th</sup> [8 days]
- Comment resolution ends on May 14<sup>th</sup>
- Eurocae virtual voting goes out a week before publishing
- Plenary Vote to Publish on May 15<sup>th</sup> [Virtual]
- Updated Report submitted to RTCA & Eurocae on May 16<sup>th</sup>
- Q2 SC-216/WG-72 Plenary week of June 9<sup>th</sup>
- RTCA PMC June 26<sup>th</sup> (fyi – doc needs to be provided 4 weeks prior)

## 2025 Meeting plans:



## 2026 Meeting plans:



- Philip Watson from Panasonic informed the group that their Irvine location was just 2 miles from John Wayne/Orange County airport (SNA) and approximately 75 minutes from LAX.
- Getting back to SG-6 topic. Nikita has prepared a diagram to show her schedule for the FAQ document.
- Industry engagement slides were posted online.
- Minutes from last meeting were approved.
- Stefan asked about the availability of plenary time to discuss the NC and H comments received in the RAC. Stefan then emphasized the importance of allocating sufficient meeting time for a virtual plenary to effectively discuss the comments.