RTCA Paper No. 310-24/SC216-156
EUR. 382-24 / WG72-182

St. Denis and Washington DC, 10/12/2024

EUROCAE WG-72 Meeting #76 / RTCA SC-216 Meeting #67 Joint Plenary **"Aeronautical Systems Security"**	
Date	***Monday – Friday 07-11 October 2024*** ***09:00 – 17:00 EDT / 15:00 – 23:00 CEST*** *Friday 11th ends at 13:00 EDT*
Place	***EUROCONTROL, Brussels, Belgium (and Virtual)***
Venue	***EUROCONTROL Headquarters*** ***Rue de la Fusée 96*** ***1130 Brussels, Belgium***
Hosted by	***Eurocontrol***

Attendance:

	Contact	Organization	OCT 07	OCT 08	OCT 09	OCT 10	OCT 11
	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	X	X	X	X
	Andrew Drake	NetJets	X	X	X	X	X
	Andrew Kornecki	ERAU	X	X	X	X	X
	Andreas Henke	DLH		X	X	X	X
	Andrea Cascio	Leonardo	X	X	X	X	X
	Aneesh Sankruth	Gulfstream					
	Angeliki Karakoliou	EASA			X		
	Anna Guegan	EUROCAE	X	X	X	X	X
	Anup Raje	Honeywell	X	X	X	X	X
	Arthur Pang	Boeing	X	X	X	X	X
	Barbara Clark	FAA					
	Ben Nagel	CyberBen	X	X	X	X	X

	Bernard Margelin	Airbus	X	X	X	X	X
	Brian Petre	GE Aerospace					
	Bill (William) Trussell	IFR Development	X	X	X	X	X
	Billy Ogunsola	CAA-UK	X	X	X	X	X
	Britney Boler	Southwest Airlines					
	Carl Schuett	Southwest Airlines					
	Cecil Deleon	Southwest Airlines					
	Charles Sheehe	NASA					
	Chris MacMullin	Department of National Defence of Canada					
	Christopher Terrington	Collins Aerospace					
	Claudio H	Lilium	X	X	X	X	X
	Cristian Bertoldi	Airbus	X	X	X	X	X
	Cyrille Rosay	EASA	X	X	X	X	X
	Dan Diessner	ERAU					
	Daniel Salter	CAA-UK		X	X	X	X
	David Chen	FAA					
	David Harvie	ERAU	X	X	X	X	X
	David Pierce	GE Aerospace		X	X	X	X
	Davide Martini	EASA		X	X	X	X
	Deepak Kamath	FAA					
	Emerson Luiz Cunha	EMBRAER		X	X	X	X
	Esha Vasdev	Department of National Defence of Canada					
	Felix Meier-Hedde	Airbus			X	X	X
	Filippo Tomasello	EuroUSC Italia					
	Francois Triboulet	EASA					
	Frédéric Heurtaux	Safran Group					
	Gabriel Elkin	MIT-LL					
	Garv Stephenson	Wisk					
	George Chang	Boeing	X				
	Gilles Thales Descargues	Thales Group		X	X	X	X
	Hagop Kazarian	Bombardier	X				
	Hannes Alparslan	EDA					
	Igor Hoffman	UAL		X	X	X	X
	Isaac Lee	Southwest Airlines					
	Isaac Rodriguez	Wisk					
	Isidore Venetos	FAA	X	X	X	X	X
	Ivan Padilla Muro	UPM Madrid	X	X			
	J.P. DeKruiff	IOActive Cybersecurity					
	Jakub Cunat	Egis Group			X		X
	Javier Diana	EUROCAE					
	Jean-Paul Moreaux	EASA					
	Jeff Burkey	FAA	X	X	X	X	X
	Jens Hennig	GAMA					X
	Johannes Goebel	EASA				X	
	John Craig - Shift5	Shift5					

	John Flores	FAA	X	X	X	X	X
	John Peace	FAA					
	Jose M. Fernandez	Polytechnique					
	Jonathan Lee (MIT LL)	MIT LL					
	Judicael Gros-Desirs	Airbus	X		X		
	Kanwal Reen	Collins Aerospace	X	X	X	X	X
	Karan Hofmann	RTCA	X	X	X	X	X
	Ken Alexander	FAA					X
	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	X	X	X	X	X
	Laurent Leonardon	Collins			X	X	X
	Lawrence Baker	NCC			X	X	X
	Lee Howard	Honeywell	X	X	X	X	X
	Logan Cummings	GE Aerospace					
	Ludovic Donnadieu	Airbus	X	X	X	X	X
	Luigi Marotta	Crisalion	X	X	X	X	X
	Luis Lozano	Ineco					
	Manon Gaudet	IATA		X			
	Marc Lord	CA Dept of National Defence					
	Marcos Ramos	Embraer	X	X	X	X	X
	Marcus Labay	FAA					
	Marcus Session	ACI/NA					
	Marie-Chantal Mouret	Airbus					
	Mario Lenitz	Austro Control	X	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	X	X	X	X
	Marty Reynolds	A4A					
	Matthieu Willm	Dassault Aviation	X	X	X	X	X
	Michael Vanguardia	Boeing					
	Michael Welch	FAA					
	Mikaëla Ngamboé	Polytechnique Montreal					
	Mickael Sabelle	Collins			X		
	Mike McCartney	FAA	X				
	Mike Noorman	GE Aerospace					
	Mike Shalvey	Southwest Airlines					
	Mike Tumminelli	Gulfstream					
	Mila Obradovic	Canada DOD	X	X	X	X	X
	Milton Santos	EMBRAER					
	Minh Trang	Airbus	X	X	X	X	X

	Mitch Trope	Garmin	X	X	X	X	X
	Nicolas Durandeau	EASA	X				
	Nikita Johnson	Rolls Royce	X	X	X	X	X
	Niv Siva	CAA-UK	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		X	X	X	X
	Phil Watson	Panasonic	X	X	X	X	X
	Phil Windust	FAA		X	X	X	X
	Philippe Dejean	Safran Group	X	X	X	X	X
	Prachi Shekhar	EGIS Group					
	Pieter Wessel	CA Dept of National Defence					
	Raphael Blaize	Thales			X		
	Richard Nguyen	Boeing	X	X	X	X	X
	Rob Segers	FAA	X	X	X	X	X
	Roland Olivier	Boeing	X	X	X	X	X
	Romuald Salgues	Airbus Helicopter					
	Rosemberg Andre da Silva	ANAC-Brazil	X	X	X	X	X
	Sam Masri	Honeywell	X	X	X	X	X
	Sarah Stern	Boeing	X	X	X	X	X
	Seth Stewart	Pratt & Whitney Canada					
	Siobvan Nyikos	Boeing	X	X	X	X	X
	Sparpano Daniele	Leonardo	X	X	X	X	X
	Stefan Schwindt	GE Aerospace	X	X			
	Stephen Van Trees	FAA					
	Tara Knight	Southwest Airlines					
	Ted Kalthoff	Archer Aviation					X
	Ted Patmore	Delta	X	X	X	X	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				X	

Day 1 Monday 10-07-2024

WG 72 and SC-216 Plenary Part 1

- Cyrille, Patrick M. and Siobvan N. opened the meeting and greeted participants
- Kristof Lamont greeted group and presented health and safety information for the facility.
- Karan Hofmann 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. Karan informed the group that recording of both video and audio of the meetings is not allowed.
- Anna presented an informational slide about Eurocae workspace hub and an upcoming RTCA/Eurocae Aviation Cybersecurity Summit scheduled for October 23rd. Several RTCA SC-216/Eurocae WG-72 members will be participating as panel members.
- Cyrille and Siobvan presented the agenda and facilitated introductions of participants around the room and online.
- Meeting minutes from the Washington DC June 2024 meeting were approved.

Regulatory Update:

- Cyrille presented EASA regulatory update:
  - Cyrille stated that there are no new EASA rules established. He added that if equipment is certified, it can be reused. However, ATM systems will require design organization approval and certification per ED 205.
  - Nicolas Durandeau mentioned that a new certification memo is available on the EASA website, which guides EASA's level of involvement in the certification process. The criteria for this involvement are based on factors such as performance, complexity, criticality, and the novelty of changes. Stefan and Nicolas provided a link for the EASA memo: https://www.easa.europa.eu/en/downloads/140011/en
  - Anup asked if a product is certified under the Cyber Resilience Act, would it still need to be mapped for approval for airborne products. Cyrille agreed that CRA evidence can be used but that it is necessary to map to criteria for airborne products
  - FAQ document to explain and clarify the use of products certified under the CRA..
- Varun Khanna presented FAA regulatory update: Varun stated that the FAA NPRM is out for comments. He added that the rule has to be out within 16 months from the end of comments (oct 21). The also mentioned that the AC is out as well. Stefan Schwindt announced that AIA is collecting comments on the NPRM and AC to ensure more seamless processing by FAA. Olivia Stella added that for operators that are A4A members, A4A will be sending a joint set of comments.
- Ken Kitamura added that there is nothing new from JCAB.
- Patrick asked about the status of DO-326B publication. Anna responded that is planned for Friday October 12th.
- Nicolas added that EASA will invoke 326B. Varun responded that its automatic, we will have to start using 326B

SG-5 DSEC:

- Olivia presented SG-5 task sheet. The objective is to create a publication that outlines minimum standards for the generation, storage, and delivery of crucial aviation data. This includes Operational Flight Programs and sensitive maintenance records.
- Olivia cited the Terms of Reference (ToR) call for a "Standard on Aviation Data Security" will detail protective measures and timelines against threats to various forms of data, including executables and databases.

- Olivia added that the Minimum Viable Product (MVP) will provide a framework for offering data security guidance tailored to different data categories, including airborne software.
- Olivia presented key document Timeline:
  - October 2024: Complete first draft and internal review.
  - November 2024: Revisions.
  - December 2024: Vote to proceed to public review.
  - March 2025: Final review and completion.
- Olivia then presented document outline and actions that SG-5 is working on including:
  - Clarify normative vs. informative sections.
  - Develop visual aids for data flow.
- Stefan advocated for a thorough coverage of all electronic data and files involved in aviation, suggesting a focus on potential safety impacts rather than just business considerations.
- Varun added that the scope of this document is for electronic transfer through the various pathways and physical security is out of scope
- Olivia updated Section 1.2 accordingly:

  All electronic data under the scope of IUEI that can be transferred in aviation including known and future data types that impact aviation safety.

- Stefan emphasized the importance of aligning with ER-013 definitions to ensure consistency and Varun advised against creating new definitions.
- Stefan suggested the need for an ER-013B in the future to complement ER-013A.
- Rosemberg noted the importance of maintaining consistency with DO-200 standards.
- Varun emphasized the importance of ensuring the security of packaging regardless of the severity level of software. He highlighted that vulnerabilities in DAL D software can eventually propagate to higher severity software, specifically DAL A, necessitating that protection measures be implemented at the highest security level.
- Kanwal then added that if the same security level is needed, there should not be a need to classify the data.
- Olivia added that we would take data classification out.
- Olivia presented the NIST cyber security framework. She explained that the framework is designed to prioritize security measures based on risk management, and facilitate communication among internal and external stakeholders
- Philip Watson from Panasonic inquired whether the appendices would hold normative information rather than serve merely as examples.
- Olivia confirmed their normative status, which prompted a discussion about the necessity of clearly distinguishing between normative and informative content within the document. Matthieu Willm from Dassault suggested explicitly indicating the normative status to prevent confusion.
- The discussion shifted to security integration in aviation data, focusing on avionics. Participants underscored the urgency for robust security measures, acknowledging shortcomings in existing practices such as Cyclic Redundancy Checks (CRC), which Stefan labeled as ineffective. Olivia pointed out that without a mandate for secure practices, there was little authority to compel manufacturers to adopt them.
- Stefan discussed the need for communication with authorities to enhance software distribution security standards across the industry. Concerns arose that lacking a defined standard might compromise software security and compatibility among operators and suppliers. The conversation concluded with mentions of technical aspects, including confidentiality measures like encryption and access controls.

Day 2 Tuesday 10-08-2024

SG-6:

- Nikita started the meeting by presenting a roadmap to the new DO-356/ED203 FAQ document submittal that included the document timeline, document structure, and team contributions and involvement. Nikita also reviewed a list of the document topics. The document will include three sections of FAQ topics grouped by categories. The three groups are managing security risk, protecting against IUEI and Detecting & minimizing IUEI.
- Document Review Schedule: In December, a comprehensive review will be conducted to identify necessary changes or additions to the DO-356/ED-203 normative sections.
- Karan has noted that the FAQ document will not be going to FRAC for approval, and therefore, must function solely as an informative document.
- Siobvan Nyikos emphasized that, due to the nature of the FAQ and upcoming Change 1, the teams working on both must ensure alignment.
- Stefan Schwindt pointed out that Change 1 has a longer lead time and should be completed first.
- TOR Date Discrepancies: The TOR outlines different timelines for FAQ and Change 1 publication: March for FAQ and June for Change 1. Stefan Schwindt raised concern over this timeline, advocating for simultaneous release.
- There was a discussion regarding the use of CRC as a security measure. Stefan Schwindt stated that CRC lacks both preimage and secondary preimage resistance, essential for security, emphasizing that CRC should only be considered for error detection. Most participants agree that CRC should not be considered as a reliable security measure and is limited to error detection use.
- Stefan Schwindt highlighted that it is essential to include information regarding the use of Cyclic Redundancy Check (CRC) as it does not fulfill security needs due to its lack of properties.
- Additional inquiries on when and how different cryptographic hashes can serve as security measures would add value in understanding effective threat intelligence.
- Properties of Cryptographic Hashes: Cryptographic hashes were designed to offer preimage and secondary preimage resistance; however, they can face various mathematical and implementation challenges that dictate their suitability for different scenarios.
- Nikita Johnson (SG6) recommended the order of topics for future discussions, including:
  - Common Criteria
  - Commercial Off-the-Shelf (COTS) products and associated NC from WG-112
  - Special Conditions for airworthiness (STC)
  - Technical Standard Orders (TSO)
  - Concerns with Common Criteria (CC)
- Stefan Schwindt pointed out that Common Criteria requirements do not consistently align with real-world attack capabilities, indicating that the framework may be outdated for contemporary security needs.
- Martin Call discussed the high costs associated with obtaining CC certification for products, indicating that it may deter some companies from seeking certification.
- There are various updates pending from ISO standards; the most current version of CC can be found on the Common Criteria portal, which is crucial for keeping abreast of changes that may not yet be reflected in ISO documentation.
- Nikita Johnson detailed EAL definitions and their levels:
  - EAL1: Functionally tested
  - EAL2: Structurally tested
  - EAL3: Methodically tested and checked
  - EAL4: Methodically designed, tested, and reviewed
  - EAL5: Semi-formally verified design and tested
  - EAL6: Semi-formally verified design and tested
  - EAL7: Formally verified design and tested
- Gilles Descargues clarified that protection profiles do not correlate directly with EALs and

suggested that a list of agreed protection profiles exists for common cases.

- The current ISO version of CC is ISO 15408-X:2022, with ongoing updates expected for ISO 15408.
- Anup Raje presented COTS SAL 3 FAQ discussion charts. The presentation titled 'Background for COTS-SAL3 FAQ discussion,' discussed achieving SAL3 for Commercial Off-The-Shelf (COTS) components. It outlines a three-step process that tailors objectives for COTS components while providing guidance on selecting, integrating, and testing these components to maintain security. The presentation also suggests collaboration between working groups to align approaches to COTS and SAL3 compliance.
- SG-6 took the action to coordinate with WG-112 to match approach for COTS
- Patrick presented a structured approach to addressing the security of legacy systems, focusing on defining and mitigating threats. It highlighted several critical factors, including the nature of attacks—specifically their manipulation of the rate, size, and content of data.
- The outlined process follows these steps:
  - Define Threats: Identifying potential security threats to the system.
  - Review Existing System: Examine requirements for constraints, isolation, and restriction based on the defined threats. This involves assessing design artifacts, reviewing design processes for peer/code reviews and coding guidelines, and tracing requirements for verification purposes.
  - Requirements Evaluation: Compare identified requirements against the outlined threats to gauge the level of mitigation achieved.
  - Gap Evaluation: Identify any gaps in security measures or process.
  - Gap Resolution: Address deficiencies in traceability or verification, potentially by adding requirements or conducting additional testing, and implementing procedural measures that support security.
- The presentation included a System Level Considerations: Consider safety mechanisms applicable to different Design Assurance Levels which can also function as security mechanisms. Recognize that systems with lower safety impact may not have implemented security measures, thus presenting new risks at the interface level. Approaches to address these risks include isolation, augmenting procedures, or updating the system.
- In a following discussion, Stefan Schwindt raised a concern regarding the use of the term "legacy" in a document, indicating that it lacked a legal definition, which could lead to ambiguities.
- Martin Call questioned whether "data content" encompassed command and control data or protocol-related information.
- Stefan emphasized the importance of aligning the current discussion about security measures with previous discussions on CRC and what constituted effective security measures. He noted that there were various elements present in both old and new systems that served as security measures, even if they did not fit the traditional IT security framework.
- Olivia Stella highlighted the subjective nature of what constituted a threat. She pointed out that individual perceptions of threats could vary widely, complicating the development of a comprehensive threat list.
- Gilles Descargues posed a question about the threshold at which modifications to a legacy product would achieve an acceptable level of robustness.
- Philip Watson provided an example of spoofing, highlighting it as a way to test the system's handling of "valid data inputs" that could lead to unintended functions, emphasizing the importance of data rate, size, and content being within expected norms.
- Gilles agreed, noting that this concept was closely aligned with the objectives of SAL1. In response, Stefan Schwindt clarified that if data is spoofed, it constitutes manipulation of data content, as it introduces incorrect information.

- Aneesh Sankruth presented potential issues with current DO-356A guidance on SAL Objective, security measure characterization and residual risk assessment. Aneesh also presented a recommended update to the guidance.
- Gilles Descargues emphasized the importance of using threat level metrics over CVSS environmental metrics for assessing risks in operational environments.
- Participants engaged in a conversation about the need to establish evidence for operational or physical controls and discussed the implications of accepting or transferring risk.
- Stefan Schwindt pointed out that protection is necessary when risks exceed acceptable levels set by authorities, while acknowledging the organization's individual risk appetite and the responsibility transferred to pilots in aviation.
- Patrick Morrissey emphasized the importance of managing residual risk as it is transferred through systems and highlighted the need for clear communication to OEMs regarding risks associated with STC integrations.
- Concerns were raised about how adding an STC could introduce safety risks, especially when security is handled only partially by non-OEM STC holders.
- Participants underscored the need for OEMs to document potential security implications of STC interactions, as this would aid operators in managing associated risks effectively.
- Varun provided a presentation titled "aircraft Systems Information Security Protection (ASISP) SAL/Level E Systems.
- Varun's presentation discussed level E systems and the need for the addition of SAL protection measures for DAL E systems.
- Varun presented that current FAA position is to not use DAL E systems to add security measures for the purpose of preventing propagation to the rest of the aircraft.
- Ted Patmore added that DO-178C 'E' pertains to airworthiness, though he noted that safety issues, including security concerns, often extend beyond airworthiness considerations. Patmore highlighted that safety issues can also arise outside of airworthiness, particularly in areas such as Air Traffic Control (ATC).
- Sankruth Aneesh emphasized the disagreement surrounding SAL and DAL arguing that serious threats can emerge from low DAL functions, citing the example of data loading processes where malicious software could potentially have catastrophic implications.
- Stefan presented slides discussing the relationship between DAL and SAL, their use and the need for the FAQ document to reevaluate existing analysis frameworks to account for both safety and security considerations effectively. While safety and security have similar goals, the architectural and process solutions are different. Therefore SAL and DAL have been defined separately and are independently assigned. For this reason, no technical relationship should be inferred. A separate issue is how visibility of security measures can be achieved for authorities when security is proposed for DAL E systems
- The SG leadership took several actions to further help the objectives.

Day 3 Wednesday 10-09-2024-SG-4, ISMS

- Siobvan presented the agenda
- Daniel Salter (UK CAA) provided a comprehensive overview of the UK Information Security Management System (ISMS) regulation as governed by the UK CAA under the Department for Transport.
- Daniel highlighted CAP1753 as the cornerstone document and indicated that the regulatory environment has largely remained stable following the UK's exit from the EU.
- Daniel detailed the alignment of the UK ISMS regulation with Part-IS objectives, alongside establishing various working groups targeting distinct regulatory areas.
- The key goals of the ISMS initiative were mentioned, mainly focusing on enhancing resilience and ensuring compatibility with global regulations.
- Rob Segers provided a presentation titled "ICAO Trust Framework Doc 10204 Manual on Information Security".

- Rob presented that the ICAO Trust Framework Document 10204 Manual on Information Security aims to enhance international confidence in information security practices among aviation organizations.The manual outlines what can be shared between organizations and adherence to standardized requirements and DAL/SAL certifications, although limitations exist regarding the detailed sharing of risk assessments. The manual presents a risk management approach that categorizes acceptable compromise likelihoods into advanced, intermediate, or basic protection levels, necessitating a collaborative response if risks exceed specified limits. The document, which will include chapters on topics like identity management, incident response, and security in software development, is in the final stages of review, with publication planned for Q1 2025.
- Adam Patrick highlighted the importance of a cohesive approach between the different groups such as ICAO, IATA, RTCA and Eurocae to contribute value to the aviation industry.
- Olivia Stella agreed on the need for clarity regarding these interconnections, while Siobvan Nyikos expressed a desire to discuss strategies to align these documents and avoid duplication.
- Frank Steunou pointed out that safety assessments are already in place for aviation facilities and infrastructure.
- Patrick Morrissey summarized that ICAO offers guidance to nations, who then choose to align their regulations, thereby facilitating international consistency through industry standards that comply with these regulations.
- Mitch Trope (Garmin) and Mario Lenitz (Austro Control) provided a presentation titled, “Small Organizations and ISMS”
- The presentation focused on identifying the unique characteristics of small and simple organizations as they relate to Information Security Management Systems (ISMS) and the challenges they face in establishing effective security measures. The aim was to propose realistic guidance and maturity models tailored for these organizations.
- This presentation provided a structured approach to understanding the specific needs and challenges of smaller organizations in developing ISMS frameworks, aiming to foster an environment conducive to compliance and enhanced information security practices.
- Siobvan discussed the importance of making the ISMS framework stand independently from Part-IS language, with objectives that support aviation-specific needs.
- She proposed moving section 2.2, "Mapping to Part-IS," into an appendix to allow ISMS to function as a standalone document.
- Siobvan outlined the next steps to review objectives and finalize them prior to the December plenary.
- Angeliki Karakoliou provided a presentation titled “Insider threat considerations”.
- Angeliki explained the importance of factoring personnel trustworthiness into risk assessments, including access control, system architecture, and anomaly detection.
- She described dual authorization, where both a manager and their supervisor approve access to sensitive areas, as a method for enhanced control.
- She emphasized that trust should not be assumed and should instead be supported by evidence-based evaluations.
- Kristof asked about managing trustworthiness if an employee’s circumstances change.
- Angeliki responded that ongoing evaluation of trustworthiness is crucial, especially in roles with security clearances.
- Nikita and Kanwal discussed ISMS Risk Management Process
- Nikita explained the ISMS risk management process, particularly its emphasis on safety-oriented assessment approaches.
- She noted that Part-IS compliance is approaching and highlighted the decision to incorporate established safety-based risk assessments into the ISMS document.
- Nikita pointed out that the Bowtie concept is used to link safety and security impacts but acknowledged that the document’s context establishment requires further work.
- Alain presented Airbus Maturity Assessment Tool for Continuous Improvement:

- Alain introduced Airbus’s maturity assessment tool, designed to help management understand ISMS maturity levels across categories aligned with Part-IS.
- The tool uses a 5-level scale to assess compliance with maturity levels, and Alain shared an example question to illustrate the assessment process.
- He mentioned that Airbus is testing the tool within approved organizations and asked if the committee saw any benefit in including a similar tool in the ISMS document.
- Tom McGoogan provided a presentation on OT Security and ISMS Integration
- Tom discussed OT Security Approach, why it matters and Part IS requirements.
- Tom highlighted the importance of addressing OT security and the need for a consistent approach to IT interfaces within ISMS guidelines.
- Tom emphasized the importance of clearly defining terms like "defect," "vulnerability," and "exploit" for proper risk management.
- Andrew expressed concern about vulnerability information and the challenges in managing risk without adequate manufacturer guidance.
- Patrick clarified that airlines are required to report vulnerabilities impacting safety, not necessarily all vulnerabilities.

Day 4 Thursday 10-10-2024-SG-3, DO-392/ED-206 Update

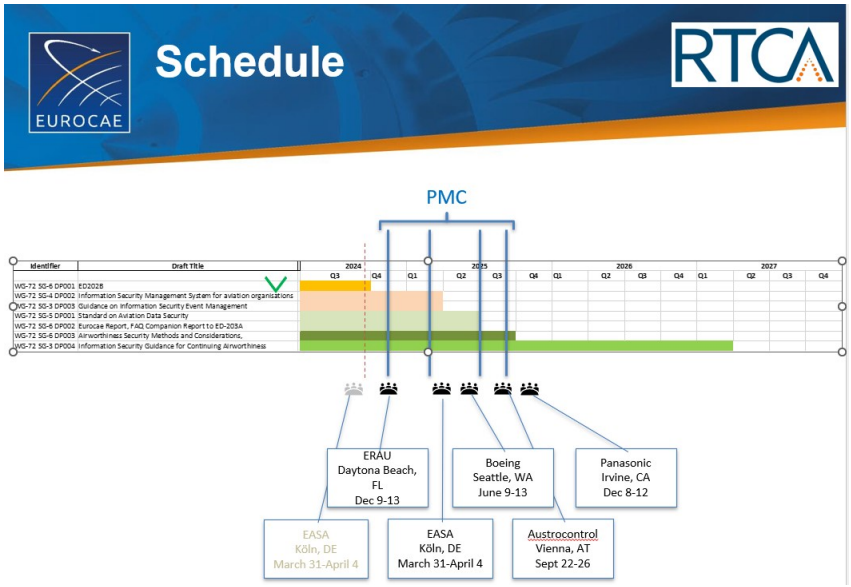
- The meeting started with a discussion on the Terms of Reference (TOR) task sheet. It was emphasized that all members should have a clear understanding of the goal.
- In a discussion about the scope of cybersecurity reporting, Olivia Stella inquired whether it applies only to ground systems, to which Marshall Gladding clarified that it encompasses both ground and airborne software.
- A review of the project timeline was conducted. The team is on track, but attention needs to be given to the approaching deadlines to ensure milestones are met without delays.
- Discussions were held regarding the interface between the ISEM and ISMS. It was noted that establishing clear communication protocols is essential for integration.
- The language surrounding the CSDS and the accompanying whitepaper was reviewed. Feedback was gathered on how best to structure this content for use. . The CSDS content will be moved into an appendix but is expected to remain distinct from the Data Sphere content currently designated for another appendix.
- The proposal regarding timeframes, distinguishing between prescriptive and objective guidelines, was discussed. Members expressed their opinions on which approach may be more efficient in achieving the organization's goals.
- The group acknowledged the need to provide comprehensive guidance on vulnerability scoring as per ED-206. Further discussions are required to ensure clarity and applicability.
- Performance requirements concerning event reporting outlined in DO-392 were also addressed. It was recognized that more structured criteria need to be developed.
- The draft document was thoroughly reviewed, resulting in substantial feedback that far exceeded previous plenaries. The presence of an editor (Marshall) is noted to enhance the quality of contributions and revisions due to an impending deadline.
- Concerns were raised about the potential for the main section content to be perceived as normative rather than informative. For example, the section on Cyber Analytical Capability could prompt inquiries from regulators regarding demonstration, which the team aims to avoid.
- Patrick Morrisey highlighted that relocating this content, rather than removing it, creates a reference point ('breadcrumbs') for employing data science in cybersecurity, aligning with the group's objectives.
- It was proposed to revise the definition of 'security architecture' in Section 2.1.2, suggesting the term 'mitigate' may be too forceful. The consensus was to use 'potentially mitigate to an acceptable level of risk.'
- CyberBen presented a definition from ER-013A. The group decided to adopt this

established definition.
- A change from 'Data Scientists' to 'Data Science Team' in Section 3.1 was agreed upon. The roles and responsibilities may also be reevaluated, potentially shifting from 'team' to specific roles.
- It was decided to use 'security environment' instead of 'security architecture' in Section 5.4.4 to better define the scope of organizational responsibilities.
- Feedback from the plenary will be consolidated into the next version (1.2) of the document, with Marshall already undertaking this process.
- SG3 has outlined the following action items for further investigation:
  - Develop the ISEM/ISMS integration language.
  - Continue discussions on vulnerability scoring, specifically concerning normative section inclusion.
  - Establish performance timelines.
- The completion date for FRAC Resolution is set for December 2024, while PMC Completion is expected by March 2025.

Day 5 Friday 10-11-24

WG 72 and SC-216 Plenary Part 2

- Opening remarks by Cyrille.
- Siobvan reminded participants that the plenary RTCA and EUROCAE rules and regulations apply for today's plenary.
- Siobvan Nyikos provided a link to an AIA paper on pen testing that was discussed yesterday...https://www.aia-aerospace.org/publications/aia-civil-aviation-cyber-security-subcommittee-testing-white-paper-2021/'
- Cyrille announced WG 72 vacancies- WG 72 is looking for a new Chair and for an EU based secretary. SG-3 is also looking for a secretary.
- Cyrille explained the effort in trying to sync up and align Eurocae and RTCA
- DO-326B will be published on the 15th of October in both the US and Europe. It was mentioned that 45 days are needed for PMC and publishing
- Rebecca Morrison mentioned that changing meeting locations outside RTCA will require additional process including audio check
- Meeting minutes for the June 2024 plenary meeting were approved.
- Next meeting dates and places for year 2024 and year 2025 were presented and updated as follows:



Subgroup status:

SG-3 Status:

- Andrew presented SG-3 status and progress made thus far including defining what is needed to move forward such as the need to define the safety risk/ impact based on the exploitability of a vulnerability, the need to update scoring and risk assessment sections. The group took the action to update ISEM/ISMS interface section, update language for vulnerability section, and flesh out objectives for timelines. The group is targeting December plenary for a proposal of final draft and the end of December for FRAC/OC.

SG-4 Status:

- Stefan and Siobvan presented the SG-4 subgroup status and progress made thus far. The subgroup had multiple presentations and discussions on the Benefit of EASA Part-IS AMC & GM, ICAO Alignment, the proportionality of ISMS for small organizations, and corporate ISMS.
- The group focused on several key topics, including the integration of audit results sharing mechanisms and minimizing audits as part of the supplier relationship outlined in DO-ISMS. Discussions included the necessity for suppliers to understand and expect Part-IS language in contracts and the involvement of third parties for added value, alongside considerations for insider threats. Additionally, the ISMS risk management process focusing on safety impact propagation, a maturity model approach for ISMS implementation, and the security interfaces between IT and operational technology (OT).

SG-5 Status:

- Olivia presented the SG-5 status and progress made thus far including a review of the ToR. There was emphasis on document timeline and minimum viable product.
- The Minimum Viable Product (MVP) will serve as a framework for providing tailored data security guidance, with a timeline that includes a draft completion by October 2024, followed by a public review vote in December and final review completion by March 2025. Proposed actions within the document include clarifying normative versus informative sections and creating visual aids for data flow.
- Discussion points raised emphasized the importance of covering all electronic data related to aviation safety, as well as aligning with existing definitions and standards like ER-013 and DO-200. The NIST cybersecurity framework was introduced, focusing on

risk management and fostering better communication among stakeholders. Issues around the normative status of appendices and the necessity for stronger data security measures in avionics were highlighted, alongside concerns about enhancing software distribution security standards across the industry. Discussions included encryption and access controls, underscoring the need for robust security practices in aviation data management.

SG-6 Status:

- Nikita presented the SG-6 status and progress made thus far including outlining the roadmap for the new DO-356/ED-203 FAQ document, detailing its structure, timeline, and contributions while highlighting topics centered around managing security risks, protecting against IUEI, and detecting/minimizing IUEI. A comprehensive review of the document's normative sections is scheduled for December, and it will function solely as an informative document since it is not going to FRAC for approval. Discussions also focused on the need for alignment between the FAQ and upcoming Change 1.
- The group covered various topics, including the definition and mitigation of threats to legacy systems, the necessity of aligning security and safety measures, and the importance of effective communication regarding risks associated with STC integrations. Participants emphasized the need for OEM documentation on potential security implications and discussed the relationship between Design Assurance Levels (DAL) and Security Assurance Levels (SAL), urging a reevaluation of existing analysis frameworks to effectively combine safety and security considerations. The actions taken by SG leadership aim to support these objectives.

Coordination with other industry groups:

- ICAO Initiatives: The ICAO Cybersecurity Panel (CYSECP) is focused on implementing an Aviation Cybersecurity Strategy and developing the first edition of the Global Cyber Risk Considerations (GCRC) Document. Upcoming meetings include face-to-face engagements for the ICAO Trust Framework Panel and the ICAO Communication Panel, with significant documentation such as the Manual on Information Security (Doc 10204) and Aviation Common Certificate Profile (Doc 10169) being addressed.
- RTCA SC-223/WG-108 will shift to Active Monitoring mode while awaiting the completion of industry validation and demonstrations, after which revisions of DO-379A and DO-404 will commence.
- The SAE G-34/WG-114 is progressing with ARP-6983 concerning development practices for aeronautical safety-related products, with input from the FAA being sought.
- ECSCG: Last meeting for the European Cyber security for aviation Standards Coordination Group (ECSCG) occurred May 15 2024. Eurocae WG- 41 is currently working on ED-128, Advanced Surface Movement Guidance and Control which includes system security considerations. Next meeting is scheduled for November 6 2024 at EASA headquarters in Cologne.
- US ACCESS: The US ACCESS WG is set to hold discussions on FAA NPRMs and software delivery standards in an upcoming meeting.
- The A-ISAC celebrates its 10th anniversary as an organization that now includes 129 companies globally. A-ISAC is rolling out free training for its members and continues to engage with government stakeholders for cyber risk management guidance.
- Agenda for the next plenary meeting will be out soon.

End of day 5.