RTCA Paper No. 201-24/SC216-154
EUR. 275-24 /WG72-180

St. Denis and Washington DC, 09/04/2024

EUROCAE WG-72 Meeting #75 / RTCA SC-216 Meeting #66 Joint Plenary

“Aeronautical Systems Security” Calling Notice

Date	***Monday – Friday 24-28 June 2024*** ***09:00 – 17:00 EDT / 15:00 – 23:00 CEST*** *Friday 28th ends at 13:00 EDT*
Place	***RTCA Headquarters and Virtual***
Venue	RTCA, Inc, 1850 18th Street NW, Suite 910 Washington, DC 20023
Hosted by	***RTCA***

Attendance:

	Contact	Organisation	June 24	June 25	June 26	June 27	June 28
	Aaron Renshaw	American Airlines					X
	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					
	Andrew Drake	NetJets	X	X	X	X	X
	Andreas Henke	DLH	X	X	X	X	X
	Aneesh Sankruth	Gulfstream					
	Anna Guegan	EUROCAE	X	X	X	X	X
	Anup Raje	Honeywell	X	X	X	X	X
	Barbara Clark	FAA					
	Ben Nagel	CyberBen					
	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					X
	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	X
	David Chen	FAA					
	David Harvie	ERAU					
	David Pierce	GE Aviation	X	X	X	X	X
	Davide Martini	EASA	X	X	X	X	X
	Deepak Kamath	FAA					
	Emerson Luiz Cunha	EMBRAER	X	X	X	X	X
	Esha Vasdev	Department of National Defence of Canada					
	Felix Meier-Hedde	Airbus	X	X	X	X	X
	Filippo Tomasello	EuroUSC Italia					
	Francois Triboulet	EASA					X
	Frédéric Heurtaux	Safran Group					
	Gabriel Elkin	MIT-LL					
	Garv Stephenson	Wisk	X	X	X	X	X
	Gilles Thales Descargues	Thales Group	X	X	X	X	X
	Hagop Kazarian	Bombardier					
	Hannes Alparslan	EDA	X	X	X	X	X
	Igor Hoffman	UAL	X	X	X	X	X
	Isaac Lee	Southwest Airlines					X
	Isaac Rodriguez	Wisk					
	Isidore Venetos	FAA	X	X	X	X	X
	J.P. DeKruiff	IOActive Cybersecurity					
	Jakub Cunat	Egis Group	X	X	X	X	X
	Javier Diana	EUROCAE					
	Jean-Paul Moreaux	EASA					
	Jeff Burkey	FAA	X	X	X	X	X
	Jens Hennig	GAMA					X
	Johannes vanHoudt	FAA					
	John Craig - Shift5	Shift5					
	John Flores	FAA					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	Cessna Aircraft Company	X	X	X	X	X
	Lee Howard	Honeywell	X	X	X	X	X
	Leonardon Laurent	Collins Aerospace	X	X	X	X	X
	Logan Cummings	GE	X	X	X	X	X
	Ludovic Donnadieu	Airbus	X	X	X	X	X
	Luis Lozano	Ineco					
	Manon Gaudet	IATA					
	Marc Lord	Canda DOD					
	Marcos Ramos	Embraer	X	X	X	X	X
	Marcus Labay	FAA					
	Marcus Session	ACI/NA					
	Marie-Chantal Mouret	Airbus	X	X	X	X	X
	Mario Lenitz	Austro Control					
	Mariusz Pyzynski	IATA					
	Mark Bucko	Boeing	X	X	X	X	X
	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					
	Mike McCartney	FAA					
	Mike Noorman	GE Aerospace					
	Mike Shalvey	Southwest Airlines					
	Mike Tumminelli	Gulfstream	X	X	X	X	X
	Mila Obradovic	Canada DOD	X	X	X	X	X
	Milton Santos	EMBRAER					
	Mitch Trope	Garmin	X	X	X	X	X
	Nicolas Durandeau	EASA					
	Nikita Johnson	Rolls Royce	X	X	X	X	X
	Niv Siva	CAA-UK	X	X	X	X	X
	Olivia Stella	SWA	X	X	X	X	X
	Pamela Davis	Southwest Airlines					
	Patrick Morrissey	Collins Aerospace	X	X	X	X	X
	Peter McNeely	Astronautics					X
	Peter Tsagaris	TCCA	X	X	X	X	X
	Phil Watson	Panasonic	X	X	X	X	X
	Phil Windust	FAA	X	X	X	X	X
	Philippe Dejean	Safran Group	X	X	X	X	X
	Prachi Shekhar	EGIS Group					
	Pieter Wessel	Canada DOD					
	Richard Nguyen	Boeing	X	X	X	X	X
	Rob Hood	Astronautics					

	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 (PWC)	PRATTWHITNEY	X	X	X	X	X
	Siobvan Nyikos	Boeing	X	X	X	X	X
	Stefan Schwindt	GE Aerospace	X	X	X	X	X
	Stephen Van Trees	FAA					
	Tara Knight	SWA	X	X	X	X	X
	Ted Kalthoff	Archer Aviation	X	X	X	X	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	X	X	X	X	X
	Valerio Senni	Collins Aerospace	X	X	X	X	X
	Varun Khanna	FAA	X	X	X	X	X

Day 1 Monday 06-24-2024

WG 72 and SC-216 Plenary Part 1

- Patrick M. and Siobvan N. opened the meeting, greeted participants
- 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 added that recording of both video and audio of the meetings is not allowed.
- Siobvan N. presented the agenda and facilitated introductions of participants around the room and online. Siobvan asked group to review minutes from last meeting so they can be approved on Friday.
- Sam M. added that minutes from April meetings were posted on RTCA and EUROCAE servers.
- Siobvan talked about expectations for the week. Discussed MVP minimum viable product-and the need to provide a standard that is usable, we have a lot on our plate, need to be mindful of scope and schedule. Try to keep last minute changes to a minimum.
- Patrick: Big part of our plan this week is to review the outcome for DO-326A/ED-202B. Need to focus on meaningful changes. Focus on comments that were previously made.
- Davide M.: Thank you to RTCA for hosting. Expectation is to resolve comments and for further ISMS developments-

- Regulatory Update:

- Davide Martini presented EASA regulatory update:
  - Davide discussed Part IS Implementation journey. He added that the Cyber Resilience Act was approved by the European Parliament on 12 March. It includes key provisions including cyber security vulnerability and incident reporting requirements.
  - Davide said that EASA has been implementing regulations, introducing approval organization and working with the European orgs to have a harmonized approach. New version of acceptable MOPS.
  - Davide also discussed an upcoming EASA Part IS workshop that will analyze use cases and share valuable lessons from early adopters and civil aviation authorities preparing for oversight activities.
- Varun Khanna presented FAA regulatory update:
  - Varun shared that the FAA Cyber security NPR will be out soon.
  - Phil added that the FAA reauthorization act includes cybersecurity for transport aircrafts. Another element is the establishment of an aviation rulemaking committee. It directed that the FAA is designated as a lead for aviation cybersecurity.
  - Canada will be following the US.
- Stefan shared a link for the European NPA: https://www.easa.europa.eu/en/document-library/notices-of-proposed-amendment/npa-2024-04
    - This is link is for an overview of the NPA 2024-04. It is a very wide update to Part 21
    - Stefan also provided a link for submitting comments: https://hub.easa.europa.eu/crt/
- Stefan asked participants to see notes from James Robinson on the comments that AIA is proposing to submit on various information security aspects of NPA 2024-04
- Davide added that Part-21 NPA objectives about cybersecurity include the following:
    - AMC 21.B.100(a) and 21.A.15(b)(6) — cybersecurity — new critical example ED

Decision 2020/006/R on ‘Aircraft cybersecurity’16 introduced the requirements to conduct cybersecurity risk assessments on various products (CS-25, CS-23, CS-27, CS-29, CS-P, CS-E, CS-APU). The cybersecurity risk assessment requires the identification of ‘threat conditions’, which are analogous to ‘failure conditions’ defined in US 14 Code of Federal Regulations Part 25.1309 and EASA CS 25.1309. However, whereas ‘failure conditions’ result from ‘unintentional causes’ (e.g. a part failure), ‘threat conditions’ result from intentional unauthorized electronic interaction and the implications for safety risk and security risk may differ (i.e. ‘low safety risk versus high security risk’ or ‘high safety risk versus low security risk’). Therefore, using the outcome of the safety assessment process to evaluate the criticality of the ‘information security’ compliance demonstration item (CDI) may lead to an underestimation of the level of risk and a misclassification of the CDI / level of involvement (LoI) required. The criticality of the ‘information security’ CDI should hence be based on the impact of the change on the items that may contribute to an unsafe condition as identified through the security risk assessment.

- Issue 32: AMC 21.B.100(a) and 21.A.15(b)(6) — cybersecurity — new critical example It is proposed that the list of examples in Section 3.3 of AMC 21.B.100(a) and 21.A.15(b)(6) be complemented with the following case: ‘the installation or activation of, or a change to, a function, component or system that, when subjected to an intentional unauthorized electronic interaction with that function, component or system, may contribute to a condition that has an adverse effect on the safety at the aircraft level’.

- Next topic was given by Anup Raje from Honeywell.

- Anup presented an NC submitted to a WG-112 plans for using COTS as a SAL 3 security measure. Anup suggested that WG-112 wait until the issue is resolved with the DO-356 FAQ document.
- The group had a discussion around COTS definition in the DO/ED documents. The group agreed that the issue is important to resolve because of VTOL. The FAA is considering ASTM F3532 for VTOL.

- SG-6 leadership change

- Siobvan introduced a Change to the SG-6 leadership, Nikita will take over chairman for SG-6 from Stefan.
- A vote confirmed the change
- Siobvan mentioned that PMC is meeting this week and the ToR will be presented and it is expected to be approved.

- Next topic: FCDI Collaborative Cyber Security Framework report presented by Laurent Leonardon/Collins Aerospace

- The framework goal is to define methods and modeling elements to develop definition for fine grain trust relations and maintain consistency and coordination across stakeholders.
- Laurent identified potential areas where FCDI’s work can be of benefit to RTCA SC-216/WG72 SG-4 and SG-5 work in ISMS, Data Sec and in other areas such as modeling different threat levels and automation of complex tasks.

- Next topic was an EASA presentation given by Davide Martini on Functional vs Supply and Operational chains.
  - The presentation provided an overview of an approach to cyber supply chain.
  - Davide provided a definition to the “operational chain” term as a collaborative effort to address operational tasks and risks to the safety of air navigation. He added that the “functional chain” is integrating the operational chain and the supply chain. This is to ensure that the interfaces between organizations are adequately protected.
  - Part-IS requires the protection of the so-called functional chains
  - Davide proposed considering the functional chain vs supply and operational chain for the development of section 2.3 in the ISMS document.

Plenary part of the meeting was concluded.

Working group meetings have started

- SG-6: DO-326B/ED-202B

- Stefan started presenting remaining comments that need agreements. Proposals to resolve these comments were worked during the meeting and an updated /reworded text was developed and agreed to by the group.
- All non concurs have been resolved and closed
- There were discussions around addressing propagation of threats, risk management, the challenges of data exchange and connectivity to threat sources, airframer responsibilities and operator responsibilities to ensure TC and STCs are secure and safe. Regulators and airframers need to collaborate to ensure that security measures are effectively communicated and implemented.
- Logical inconsistencies in diagrams will be fixed
- Varun expressed interest in clarifying that an applicant will clearly show that they are taking credit for security in a lower criticality system. FAQ document has been chosen to address this request.

End of day one.

DAY 2 Tuesday 06-25-2024

- SG-6: DO-326B/ED-202B-continued

- Stefan continued presenting remaining comments that need agreements. Proposals to resolve these comments were worked and an updated /reworded text was developed and agreed to by the group.
- There were discussions around the challenges of maintaining system assurance levels in environments where the Design Assurance Level (DAL) is low. Specifically, it highlights the need to isolate SAL3 components from lower assurance levels to ensure security measures are effective. The difficulty lies in demonstrating this isolation. Using higher assurance elements like EAL hypervisor can help, but the effectiveness depends on the protection profile of the evaluated security function.
- Kanwal added that this guidance is intended to be applied throughout an aircraft's entire lifecycle—from design and in-service phases to disposal. It is advised to implement this guidance during the design phase to ensure it is effective in later stages. If changes are

made to an aircraft and previous security documentation is missing (e.g., the aircraft was not certified with specific security conditions), the document offers instructions for determining applicable security objectives for those changes.

End of day two.

Day 3 Wednesday 6-26-24

- SG-3: DO-392A/ED-206A

- SG-3 status presentation was delivered by Andrew Drake from NetJets.
- Andrew pointed to the difference between the European version and the US version of the task. He presented the SG-3 group progress and planned work.
- Andrew presented current objectives for section 5.4 Vulnerability Analysis, and new proposed objectives that include a Vulnerability scoring system.
- Rob Segers (FAA) added that scoring does not mean much unless you understand the safety risk. CVSS today is for the impact on the asset but does not take into consideration the environment around the asset.
- Nekita said that they had experience that CVSS didn’t line up with their system where adjacent equipment looks different than adjacent aircraft.
- There was a discussion that clarifies that the Common Vulnerability Scoring System (CVSS) is not a risk assessment tool. Organizations can use threat level definitions from aircraft standards (ED-203A / DO-356A) as references for establishing threat criteria, and CVSS can also be used. While ED203A's threat levels are suitable for aircraft, they may not be practical for Information Security Management Systems (ISMS). The discussion suggested focusing on developing a framework for vulnerability risk assessment and emphasized that the goal is to assess risk rather than just relying on numerical scores.
- Rob S added that the correlation between the safety risk and the vulnerability is important. This what u can use to communicate between safety and security.
- Davide added that EASA would like to see scoring to provide impact on safety. From practical perspective, once u established exploitability and the impact on safety, we are interested in making sure this vulnerability is not forgotten. Any scoring should be explained to authority, they need to link it to the safety assessment.
- Andrew proposed the following:

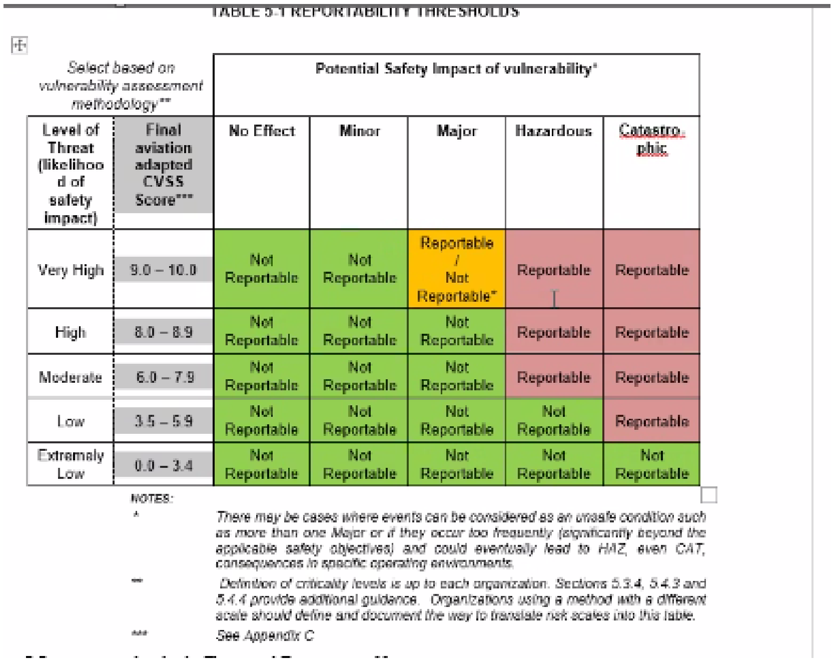


TABLE 5-1 REPORTABILITY THRESHOLDS

*Select based on vulnerability assessment methodology***		Potential Safety Impact of vulnerability*				
Level of Threat (likelihood of safety impact)	**Final aviation adapted CVSS Score*****	**No Effect**	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Very High	9.0 – 10.0	Not Reportable	Not Reportable	Reportable / Not Reportable*	Reportable	Reportable
High	8.0 – 8.9	Not Reportable	Not Reportable	Not Reportable	Reportable	Reportable
Moderate	6.0 – 7.9	Not Reportable	Not Reportable	Not Reportable	Reportable	Reportable
Low	3.5 – 5.9	Not Reportable	Not Reportable	Not Reportable	Not Reportable	Reportable
Extremely Low	0.0 – 3.4	Not Reportable	Not Reportable	Not Reportable	Not Reportable	Not Reportable

NOTES:

* *There may be cases where events can be considered as an unsafe condition such as more than one Major or if they occur too frequently (significantly beyond the applicable safety objectives) and could eventually lead to HAZ, even CAT, consequences in specific operating environments.*

** *Definition of criticality levels is up to each organization. Sections 5.3.4, 5.4.3 and 5.4.4 provide additional guidance. Organizations using a method with a different scale should define and document the way to translate risk scales into this table.*

*** *See Appendix C*

- Davide commented that the matrix should show Level of exploitability in the context of system architecture etc. vs the impact on safety.
- There were discussions that centered on integrating safety and security measures. Key points include:
    - Unique Scoring Methods: Organizations have different scoring methods, and there's interest in adapting existing safety methods for security scoring
    - Exposure and Likelihood: Exposure should be considered a part of likelihood in risk assessments.
    - Guidance and Exploitability: There is a need for clear guidance on determining exploitability levels and a concern about the lack of and consistency with safety practices.
    - CVSS and Adaptation: While CVSS is useful for measuring severity, it needs adaptation to account for physical and operational procedures. The integration of CVSS scores with safety matrices, such as those in DO-356 and Part 21.A.3, is crucial but should be balanced with a comprehensive assessment that includes architecture and attack characteristics.

- The reporting topic was discussed, and Davide noted that authority and maybe others in the supply chain/customers/other users should be part of reportability.
- There was a discussion around a need for ISEM to guide how events are evaluated for risk and reportability. Security incidents should be reported, but not all stakeholders are obligated to report directly to regulators; suppliers often report to OEM integrators first, with subsequent decisions on regulator reporting. Organizations should use existing processes for reporting incidents and vulnerabilities if available. If not, they need to create one. Reporting for incidents and vulnerabilities in aircraft versus those in the ISMS scope should be treated differently to avoid overwhelming authorities with IT security incident reports. Reporting should consider the distance from the aircraft.
- Andrew asked the group to review the draft document.
- **ACTION:** Patrick volunteered to put together a presentation on how they do reporting
- **ACTION:** Mario will take a shot at it from Euro Control perspective.
- **ACTION:** Marshall will do a Boeing perspective.

- SG-5: DO-DSEC/ED-DSEC

- SG-5 status presentation was prepared by Olivia Stella/SWA and Alessandro Oteri/Leonardo.
- SG-5 objective is to create a new document outlining minimum standards for generating, storing, and delivering aviation data, including Operational Flight Programs, sensitive maintenance records, and other security-relevant data. The standard will detail technical requirements and timelines to safeguard data from malicious threats.
- The group is in the process of finalizing the framework and document sections, and agree on the timeline for drafting, reviewing, and publishing.

End of day three.

Day 4 Thursday 6-27-24

- First topic was on Finnair perspective on Part-IS (and NIS2) compliance approach. A presentation was given by Erka Koivunen and Timo Arndale from Finnair.

- Approach used a common responsible person, common ISMS, and common cyber security/information system risk development program.
- Cyber program was incorporated within Finnair strategy execution and within workstreams.
- Members of the safety org participate in the security risk assessments and security risk findings are being shared with the safety team. Security incidents and vulnerabilities findings are also shared with safety.
- Risk assessment is used to identify and control supply chain risk. Finnair is looking at using protection level agreements with supply chain partners based on the requirements. Requirements may include lifecycle controls. For example, role-based lifecycle. New employee started with the company may need different control than an employee that has been there fo a long time. Same applies to newly collected data to decommissioning. Supplier management also has a lifecycle.
- Davide asked how assumptions are made for the lifecycles, interfaces, protection elements and how risk posed to anther org outside Finnair is being considered.
- Timo responded that they manage this with the risk assessments.
- The presentation continued discussing Finnair approach in improving disaster recovery and fail-safe practices. The presentation emphasized continuity of critical operations and maintaining safety.
- Siobvan asked what do you want to see in the ISMS document? Timo responded that the top 3 items they like to see in the ISMS are: the scope of ISMS, (how manage scope), risk management is a second, then supply chain management is a third.

- Second topic today is a presentation on Part-IS from Dassault given by Mathew:

- Mathew’s prestation discussed part IS interface type such as supplier, customer, etc., criticality of interface, as well as risk assessment of the interface.

- Third topic today is a presentation on Part-IS from Lufthansa given by Andreas Henke:

- Andreas’s presentation discussed their part IS pilot project in creating an Information Security Management Manual (ISMM) to connect between ISMS and SMS. A proposed table of content/outline was presented.

- Fourth topic today is a presentation on Part-IS from Rols Royce given by Nikita:

- Nikita presented Rols Royce version of ISMM. A proposed table of content/outline was presented.
- Nikita added that it has been helpful to use the ISMM for auditing compliance and monitoring compliance.
- Rols Royce is using 80 percent of exiting processing including existing airworthiness processes with added security scope.
- Supplier management is covered in the same manual by pointing to an entire framework that deals with supply chain.

- Next topic is DSEC by Olivia Stella, Alessandro Oteri:

- Olivia reviewed the ToR and reminded the group that the focus of the document was to provide data security based on the type of data. A stretch goal to add 3 use cases related to airborne software, aircraft database and aircraft logs was presented.
- Olivia presented a framework review that included data flow and interfaces and security objectives in an aviation product life cycle.
- The group had few suggestions about the framework to ensure it is comprehensive and includes a specific use case/example, not just limited to software data categories.
- It was suggested that the framework applies to systems beyond certified airborne systems (DAL D+).
- It was also suggested to consider revising the structure by addressing "What" before "Where" and renaming the title to "Determine Interfaces and Data Flow."

End of day Four.

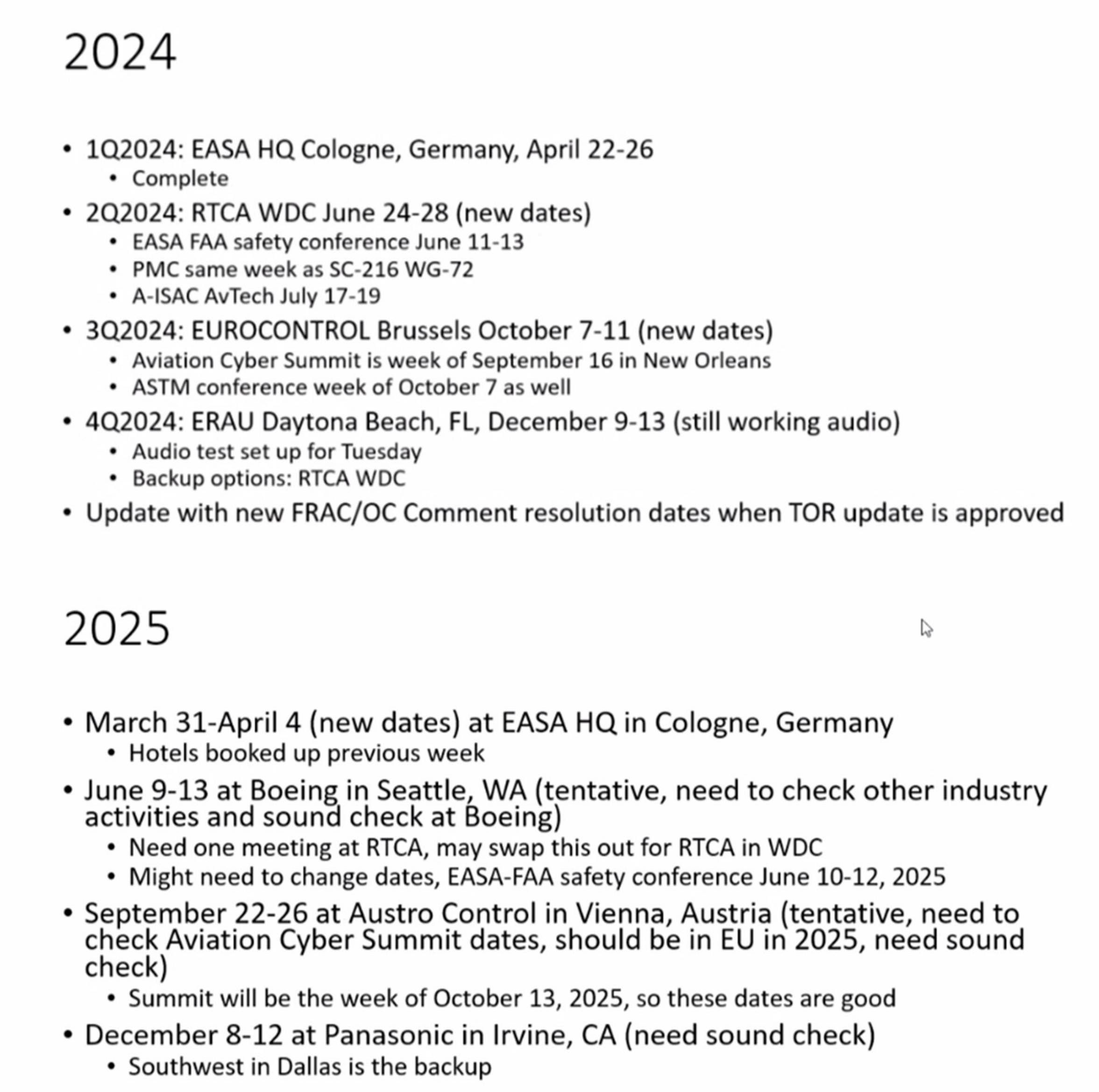
Day 5 Friday 6-28-24

WG 72 and SC-216 Plenary Part 2

- Opening remarks by Patrick.

- Siobvan reminded participants that the plenary RTCA and EUROCAE rules and regulations apply for today’s plenary.
- A vote was conducted for DO-326B to go to the PMC and Council for approval and publication. All voted in favor of publication.

- Next meeting dates and places for year 2024 and year 2025 were presented and updated as follows:



2024

- 1Q2024: EASA HQ Cologne, Germany, April 22-26
  - Complete
- 2Q2024: RTCA WDC June 24-28 (new dates)
  - EASA FAA safety conference June 11-13
  - PMC same week as SC-216 WG-72
  - A-ISAC AvTech July 17-19
- 3Q2024: EUROCONTROL Brussels October 7-11 (new dates)
  - Aviation Cyber Summit is week of September 16 in New Orleans
  - ASTM conference week of October 7 as well
- 4Q2024: ERAU Daytona Beach, FL, December 9-13 (still working audio)
  - Audio test set up for Tuesday
  - Backup options: RTCA WDC
- Update with new FRAC/OC Comment resolution dates when TOR update is approved

2025

- March 31-April 4 (new dates) at EASA HQ in Cologne, Germany
  - Hotels booked up previous week
- June 9-13 at Boeing in Seattle, WA (tentative, need to check other industry activities and sound check at Boeing)
  - Need one meeting at RTCA, may swap this out for RTCA in WDC
  - Might need to change dates, EASA-FAA safety conference June 10-12, 2025
- September 22-26 at Austro Control in Vienna, Austria (tentative, need to check Aviation Cyber Summit dates, should be in EU in 2025, need sound check)
  - Summit will be the week of October 13, 2025, so these dates are good
- December 8-12 at Panasonic in Irvine, CA (need sound check)
  - Southwest in Dallas is the backup

- Meeting minutes for the April 2024 plenary meeting were approved.

- Next Topic was Subgroup status:

- SG-3 Status:
- The subgroup presented their 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 is looking for volunteers to help draft a section on who is responsible for vulnerability and incident management of different assets.
- Alain added that Airbus plans to present their version of CVSS to the group during the upcoming meetings.
- SG-4 Status:
- The subgroup presented their status and progress made thus far. The subgroup had presentations and discussions on ISMS and risk assessments. The group will focus on meeting deadlines. The group will start creating material and possibly let the document evolve organically. There is a need for a smaller working group to check mappings to ISO-27000 for suitability with Part-IS and to address gaps in risk assessment and supply chain management. The group highlighted the importance of ISMS in satisfying

stakeholder needs and in adapting ISO 27000 for aviation. There's substantial work ahead, but the group has a solid foundation to build upon.

- SG-5 Status:
- The subgroup presented their status and progress made thus far including a review of the ToR. There was emphasis on document timeline and minimum viable product. The group discussed the DSEC framework and next steps required. The group called out for volunteers to help in the writeup.
- SG-6 Status:
- The subgroup presented their status and progress made thus far including resolving comments and a vote to allow the updated DO-326B to go to publishing. Nikita Johnson was nominated as the new EUROCAE chair for SG-6. Patrick volunteered to serve as the secretary for the group. Ben was volunteered to serve as a document editor. The group will now start work on the DO-356 FAQ project. The document will serve as a companion to ED-203A/DO-356A. A list of topics for the DO-356 FAQ project was presented. There was an agreement that regulators involvement in the development of the "FAQ" document will be important as regulators can share real certification experiences and perspectives on many of the document topics.
- RTCA director, Robecca Morrison, came by to explain that they encourage SC-216 committee to be at RTCA HQ at least once per year.

- Next Topic was Coordination with other industry groups:

- Siobvan presented status on SAE G-34/WG-114 AIA AI/ML in aviation committee. The group plenary was conducted 11-14 March 2024. SAE want AI to be handled by G-32
- Stefan presented status on ICAO Cyber related standards. Several standards/manuals were delivered including a Manual of Security Services, a Manual of security Risk Assessment, and a Manual of PKI Policy for Aeronautical communication. ICAO nations will be meeting in December 2024 in Oman. ANAC has submitted a paper on info sec and it references SC-216 DO/ED industry standards. Spec42 is a company that is heavily involved and is shaping the ICAO policy.
- Siobvan presented IPS Subcommittee status. ARINC 858P1/P2/P3 approved to publish and includes security. RTCA SC-223/WG-108 Aviation profiles for IPS rev A in FRAC.
- Olivia presented the status on ARINC SAE A4A. The group is working on a position paper D301.
- Mitch presented the status on ASTM WK82426. The group developed ASTM F3532-22 that was formally accepted by the FAA. The group is trying to address concerns from EASA with the hope to get that done by the summer.
- Other status slides were presented for ATA Spec 42, ECSCG, US ACCESS, A-ISAC, CSCAT, ERAU, and ICNS
- Agenda for the next plenary meeting will be out soon.

End of day 5.