RTCA Paper No. 103-23/SC216-142
EUR. 214-23 / WG72-169

St. Denis and Washington DC, 05/16/ 2023

EUROCAE WG-72 Meeting #70 / RTCA SC-216 Meeting #61 Joint Plenary

"Aeronautical Systems Security" Calling Notice

Date	***Monday – Friday 17-21 April 2023*** *09:00 – 18:00 CEST / 03:00 – 12:00 EDT*
Place	***Cologne, Germany (and Virtual)***
Venue	EASA Konrad-Adenauer-Ufer 3, 50668 Koln, Germany
Hosted by	***EASA***

Attendance: (P – In Person / X – Remote)

	Contact	Organisation	April 17	April 18	April 19	April 20	April 21
AR	Aaron Renshaw	American Airlines					X
	Adam Patrick	Rolls-Royce					X
AW	Adrian Waller	Thales	X	X	X		X
AC	Alain Combes	Airbus	P	P	P	P	X
AD	Andrew Drake	NetJets	P	P	P	P	P
AB	Andy Boff	Egis Aviation	X				
AG	Anna Guegan	EUROCAE	X	X	X	X	X
AR	Anup Raje	Honeywell	P	P	P	P	P
	Ben Nagel	CYBERBEN	P	P	P	P	P
	Bernard Margelin	Airbus				X	
	Bill Trussell	IFR Development	X	X			X
	Chris Rawden	Rolls Royce	X				
CR	Cyrille Rosay	EASA	P	P	P	P	P
	David Harvie	ERAU	X	X	X		X
DP	David Pierce	GE	P	P	P	P	P
	Davide Martini	EASA	X	X	P	P	X
	Felix Meier Hedde	Airbus	X	X	X		
	Garv Stephenson	Wisk	X				
	Gilles Descargues	Thales Group			X		
	Hannes Alparslan	EDA	P	P	P	P	P
JPM	Jean Paul Moreaux	EASA	P			P	
	John Flores	FAA	X	X	X	X	X
	Jonathon Bailey	Thales Group					
	Jose Romero-Mariona	RTX	X	X	X	X	X
	Kanwal Reen	Collins	P	P	P	P	P
KH	Karan Hoffman	RTCA	X	X	X	X	X
	Kevin Knott	TSA			X		
	Kevin Meier	Cessna Aircraft Company	P	P	P	P	P
KL	Kristof Lamont	EuroControl	P	P			

	Laurent Leonardon	Collins Aerospace	P	P	P	P	X
	Ludovic Aron	EASA			X		
	Mariusz Pyzynski	IATA	X	X		X	
	Mark Kelley	AVISTA	X	X	X	X	X
	Marshall Gladding	Boeing			X		
	Matthieu Willm	Dassault Aviation	P	P	P	P	X
	Mike Tumminelli	Gulfstream	X	X	X	X	X
	Mitch Trope	Garmin	P	P	P	P	P
	Nicolas Leclercq	Thales Group			X		
	Olivia Stella	Southwest Airlines					X
PM	Patrick Morrissey	Collins	P	P	P	P	P
	Peter McNeely	Astronautics	P	P	P	P	P
	Philip Windust	FAA	P	P	P	P	P
	Phillip Watson	Panasonic Avionics	X		P	P	P
	Philippe Dejean	Safran			P	P	P
	Prachi Shekhar	EGIS Group	X	X			
	Romuald Salgues	Airbus	X	X	X		X
SM	Sam Masri	Honeywell International	P	P	P	P	P
SSB	Sarah Stern	Boeing	P	P	P	P	P
SN	Siobvan Nyikos	Boeing	P	P	P	P	P
	Sophie Laborde	Thales Group	X	X			
SS	Stefan Schwindt	GE Aerospace	P	P	P	P	P
	Steven Rines	ARINC/Engenui LLC			X		
	Tara Shawde Brown	WNCO	X	X		X	
TK	Ted Kalthoff	NIAR	X	X	X	X	
	Ted Patmore	Delta Airlines	X	X	X	X	X
	Thuc Nguyen	EUROCAE			X		
VK	Varun Khanna	FAA	P	P	P	P	P
	Xidong Xu	Boeing	X		X	X	

Day 1 – 17 April, 2023

- WG 72 and SC-216 Plenary Day 1, 04-17-2023:

- Cyrille Rosay opened the meeting, greeted participants
- Gian Andrea Bandieri greeted and welcomed participants to EASA
- SC-216 Announcement by Dave & Karan:
    - Siobvan has been selected to co-chair committee with Patrick.
    - Karan presented the RTCA recognition thank you special certificate to Dave for his service to the SC-216 committee
- Karan Hofmann presented the RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, participation and membership policies.
- Cyrille and Patrick presented WG-72 , SC-216 and subgroups leadership Org Structure charts
- Sam Masri volunteered to fill the editor position for SG-3.
- Cyrille presented the agenda and facilitated introductions
- Meeting minutes from the December 2022 Plenary were accepted
- Andrea Bandieri presented EASA regulatory update:
    - EASA's "Part IS" is a piece of regulation was introduced to protect aviation safety from cyber risk. Regulation is scheduled for implementation on Feb 22, 2026.
    - Part IS includes information security incidents management requirements. 72 hours reporting requirement is counted from time of event. EASA will work with you if in good faith you need more time. Report when you become aware. Philip Watson and others expressed concern that often an event is not discovered until months later. So requirement should be "when discovered" as a security incident with an impact on safety.
    - Regulation will apply to European certification. Implementation depends on the type certificate an applicant is holding today. Applicants need to comply with part IS to keep certificate
    - If you don't comply there are 3 types of findings: Level 1 -must fix right away for safety reason, Level 2 – Up to 3 months' time provided to comply, Level 3 – Observation
    - ISMS under part IS to monitor and minimize safety risk
    - Activities EASA is doing to support Part IS implementation include a pilot program that is being used as a proof of concept
- Varun Khanna presented FAA regulatory update:
    - Cyber security rule to be published towards the end of 2023.
    - AC will be published at the same time. AC is equivalent to the European AMC.
    - FAA and TSA working to deconflict cyber incident reporting timeline requirements amongst other areas. HR-9709 gives exclusive rulemaking authority to the FAA for assuring civil aviation cybersecurity.
    - The FAA took steps to establish an Aviation Rulemaking Committee (ARC) for SMS in order to develop regulatory requirements for implementing an SMS by all Part 121 air carriers in the United States. The final rule became 14 CFR Part 5, and requires all U.S. Part 121 air carriers to implement an SMS according to requirements set forth therein as of March 9, 2018
- Siobvan and Varun presented feedback on the use of the RTCA guidelines. A number of issues users may experience when implementing the current RTCA/EUROCAE standards as a means of compliance. Potential solutions were discussed. In some cases it wasn't clear that certain chapters within the DO-356A documents were provided as informative material and not normative. Insight can be used to improve documents.

- FAA-EASA asked committee to develop a companion “FAQ” document to help address issues since updating DO-356B will take time. Using COTS and open-source security measures will be included. Timeline to be announced in June Plenary

- SG4 ISMS Information Security Management System

- Stefan presented agenda for the sub group
- White papers can be used to develop material for the ISMS, but it doesn’t have to be complete to bring it forward. Focus on safety related and safety critical items in order to satisfy part-IS. Provide guidelines that can easily translate the actions performed for part-IS into actions done for business reasons
- Question on how to address risk from organizations not following same guidelines
- Link to template that also provides a suggested format was provided
- Cost of implementing ISMS was brought up as a potential concern
- Document needs to address industry concerns
- Ensure consistent security across supply chain
- Part IS requires ISMS. AMC guidance material is out for stakeholder review. A link was provided. The term "stakeholder" in the context of an EASA was explained to include EASA Advisory Bodies (MAB and SAB) as well as FAA, TCCA, CAA Israel, ANAC (CAA Brazil)
- Jean-Paul Moreaux of EASA presented a proposed perspective on how ICAO may address cybersecurity in 2023.
- ICAO operates on “working papers” presented and agreed/rejected in ICAO plenary sessions
- Working paper could be presented by industry to request coordination with SC-216/WG72
- Ted Patmore added that all operators within the ICAO member states are required to implement a Safety Management System (SMS). This was as a result of Amendment 33 of Annex 6 to the Chicago Convention and applies to all member states of ICAO. The minimum requirements by ICAO for the SMS were as follows:

1) Identifies safety hazards.
2) Ensures that remedial action necessary to maintain an acceptable level of safety is implemented.
3) Provides for continuous monitoring and regular assessment of the safety level achieved.
4) Aims to make continuous improvement to the overall level of safety in the United States.

- The FAA took steps to establish an Aviation Rulemaking Committee (ARC) for SMS in order to develop regulatory requirements for implementing an SMS by all Part 121 air carriers in the United States. The final rule became 14 CFR Part 5, and requires all U.S. Part 121 air carriers to implement an SMS according to requirements set forth therein as of March 9, 2018
- End of day one

Day 2 – 18 April, 2023

- SG4 ISMS Information Security Management System continued-

- Other industry Cybersecurity guidance principally focused on awareness and secure operations and not on safety
- Felix Meier-Hedde presented charts on Part IS risk assessments at Airbus
- Airbus preferred method for information security risk assessments is Agence Nationale de la Sécurité des Systèmes d'Information ANSSI EBIOS Risk Manager
- Develop a customized risk assessment method for Part IS (common across Airbus)
- Adapt to Part IS where needed
- Felix provided examples for information security breach (loss of integrity, availability, confidentiality, authenticity) with potential impact on aviation safety:
- An on-board safety function is degraded.
- Loss of capability to detect, understand or handle a safety relevant issue (regardless of its cause).
- Delivering a product or service that is unsafe to operate or use (incorrect, incomplete)
- Delivering of a product or service that is insecure to operate or use (has vulnerability).
- Non-delivery of a product or service.
- Disclosing information that could be exploited in an attack.
- Using a non-authentic product or service of another organization.
- The product or service is not coming from the organization it is supposed to come from (e.g., counterfeit parts, rogue software)
- The product or service is not qualified for use (e.g. draft version, item did not pass QG)
- Exposing a safety relevant asset (from another organization)
- Considerations:
- Part IS is information security, but the safety impact may materialize on a physical part.
- Contribution to a safety scenario may be indirect.
- Risk assessment should consider:
- Risks in the assessed process
- Downstream detection means: If security breach is detected and corrected downstream, there is no safety effect.
- Upstream risks: If an input is received already compromised, the risk may be passed to downstream
- Need for a common understanding of what a 'potential impact on aviation safety' is and how the impact should be rated
- Matthieu Willm/Dassault presented Part-IS Risk assessment, Distance to safety effect- preliminary considerations
- Part-IS risk assessment security perimeter generally doesn't include the actual safety effect and the actual safety effect might even be in a different organization.
- Threat conditions, threat scenarios and risks are evaluated locally and do not consider further steps and delays beyond the security perimeter necessary to trigger the actual safety effect
- The likelihood of the global threat scenario, from the tampered asset up to the safety effect along the whole functional chain should take into account the« distance» from the local threat scenario to the actual safety effect (# of hops, timeframe, ...)
- There was a discussion on security controls effectiveness (technical and non technical controls), risk assessment coordination and ISMS integration into the SMS, and how to identify people part and technology, training and management, data security integration, to confirm what is the type of data we need and data flow, to make sure we feed data security, safety integration, involve safety and SMS and safety process. How do we feed safety knowledge into our process and expectation.

Maybe include other management systems or existing policy:

- Stefan: Need to update scope. We shouldn't tell people how to structure their organization. We can provide guidance on where good overlap may exist between SMS and ISMS. There is overlap in managing competencies. Other areas have little to no overlap.
- Patrick: As the ISMS "system" is described, it'll have to be characterized with "independent" and "integrated" examples. Objectives need to be common.
- Kanwal: If we have both examples, will it be confusing?
- Stefan: We can't assume what will be in an SMS. Maybe say "you can have an SMS, here's where they might line up, but don't assume an SMS automatically gives you security."
- Mitch: Must include proportionality in this group
- Matthieu: Do we want to build another ISMS standard, or would it be better to explain integration of the safety point of view for IT personnel?
- Kanwal: We'll have to tie IT and SMS using product security. We won't be able to change what IT is doing. We'll take credit for what's out there that they already do.
- Stefan: Some IT policies may not be acceptable once the bar is set, that's the brutal reality. Some things that are fine for business risk won't work in the safety context. Generally, we can't do something super-special for safety when assets have both business and safety risks. ISO 27001 is a good baseline, but has weaknesses. It doesn't have mandatory reporting, which we need.
- Varun: You won't have the clout to make global changes
- Patrick: Sounds like there is some "violent agreement" here. Lots of approaches and methods, also some limitations.
- Jean-Paul: Scope on the slide may not be sufficient for all the opinions being consolidated. Take more time now to define this.
- A link to the FAA and EASA SMS is provided: Federal Aviation Administration (2023). Safety management system. https://www.faa.gov/about/initiatives/sms/explained/basis Safety Management Systems, 14 C.F.R. § 5 (2023). For EASA https://www.ecfr.gov/current/title-14/chapter-I/subchapter-A/part-5
- Ted Patmore uploaded a short document Pillars_of_SMS to the SG4 Eurocae Documents as material for thought about the structure of an SMS related to aviation https://eurocae.sharepoint.com/sites/strato/34fd374d-a1c8-e811-8154-e0071b66a0a1/d07cc886-a856-ed11-bba2-000d3adea767/SitePages/Documents.aspx
- Need to have compliance monitoring functions. Delegating security tasks by accountable manager to staff. Competence and trustworthiness required from/for staff.
- Can delegated people be outside the EU for EU orgs?
- Traceability required to ensure compliance to part IS. Discussion around part IS compliance if security work is done outside the us.
- Make sure that the data is actionable.
- Your process for EU offices has to meet part IS
- Look for the type of data that is associated with safety critical systems.
- Changes to ISMS need to be approved by authority. There are exceptions for exceptional circumstances. Change impact analysis of your ISMS Be consistent with what is already there in terms of requirements.
- Discussion around continuous improvement. To reduce rise. Process should be in place to improve the system. We haven't started to discuss performance based auditing. One example is called level of involvement, different criteria, capability of org. some guarantee from that. Audit focus also can be used. Org not compliant yet, maturity can be used to bring them up to acceptable level.

Day 3 – 19 April, 2023

- SG6 DO-326A/ED-202B
  - Sarah Stern led the discussion and presented status charts
  - Sarah is trying to get different perspective from operators and other STC houses. Mitch T. volunteered to develop a presentation about their STC CIA process. Southwest may also provide an input on how it works in practice
  - Sarah presented guiding principals for a good CIA process that can be plugged into a system CIA process
  - Tara Brown added that there are several types of analyses Southwest Airlines use for change management and SMS. Southwest has developed processes to ensure controls are effective through audits, voluntary EE reporting, digital data (FOQA – from the aircraft, scheduling data etc.)
  - Sam took the action to develop a list of questions that can be used in a security CIA to help in assessing security changes. Patrick and Dave to provide input to Sam.
  - Romuald Salgues added that in the context of a product information security risk assessment (PISRA), a change that may introduce the potential for unauthorized electronic access to a systems should be considered to be 'major' if there is a need to mitigate the risks for an identified unsafe condition. The following examples do not provide a complete list of conditions to classify a modification as major, but rather they present the general interactions between security domains. Examples of modifications that should be classified as 'major' are when any of the following changes occur (extract from Appendix A to GM 21.A.91 Examples of Major Changes per discipline):
    - A new digital communication means, logical or physical, is established between a more closed, controlled information security domain, and a more open, less controlled security domain. For example, in the context of large aircraft, a communication means is established between the aircraft control domain (ACD) and the airline information services domain (AISD), or between the AISD and the passenger information and entertainment services domain (PIESD) (see ARINC 811).
    - As an exception, new simplex digital communication means (e.g. ARINC 429) from a controlled domain to a more open domain is not considered as major modification, if it has been verified that the simplex control cannot be reversed by any known intentional unauthorized electronic interaction (IUEI).
    - A new service is introduced between a system of a more closed, controlled information security domain and a system of a more open, less controlled security domain, which allows the exploitation of a vulnerability of the system
    - Cyrille provided a link to a procedure that describes how European Union Aviation Safety Agency (EASA) discharges its responsibilities for certification activities of aeronautical products within its remit. It applies to the type certification of EU aeronautical products and to changes/repairs thereto, in accordance with Annex - Part 21 to Commission Regulation (EU) No. 748/2012: https://www.easa.europa.eu/en/document-library/certification-procedures/airworthiness-type-design
  - Mike Tumminelli asked how do we merge Cybersecurity for Propulsion Systems Draft SAE AIR7368?
  - Discussion around security requirements for EFBs. Where can users find these requirements. Flight standards has operational controls on EFBs. ED 273 has requirements for securing EFBs. AMC-2025A also includes guidance for EFBs. AC-120-76D also has guidance.
  - Ben added that there was an EFB issue from about 2 month ago. EFB SW provided

faulty weight information, some pilots caught it during transfer to FMS, but some didn't.

- Cyrille added, The safety assessment of the EFB data connectivity installation should include an analysis of vulnerabilities to new threats that may be introduced by the connection of the EFB to the aircraft systems (malware and unauthorized access) and their effect on safety. This assessment should be independent and should not take any credit from the operational assessment of EFB system security, which is intended to protect EFB systems themselves. Also: the failure conditions associated with the reception of erroneous PED/EFB data have criticalities that are not higher than minor
- Sarah added that AC 120-76E (out for FAA internal comment in June 2022) will have a new section specifically addressing cybersecurity issues as well as AC 20-173A
- Editorial items to change were presented for DO-356A and DO-326A.
- TSA Presentation was given by Kevin Knott-TSA:
  - Operators are required to do a self-assessment of their infrastructure. Critical systems are IT and OT systems. Excluding aircraft systems.
  - Reporting policy requires reporting incidents within 24 hours of knowing and determining that it was a cyber incident, if it created an operational disruption.

- SG5 DO-DSEC - Data Security

- Hannes Alparslan led the discussion and presented rational for the document
  - Increasing digitalization and connectivity in aviation
  - Information security for the exchange of data between the individual systems becoming paramount
  - ED201A/DO-391 has a discussion on security for supply chain. Need a master minimum requirements for min, medium and high security levels for data security.
  - Data at rest require protection
  - Security controls for data include Physical control, Technical controls and Procedural controls
- Siobvan Nyikos and Marshall Gladding from Boeing presented SC-236 WG 96 Wireless Avionics Intra Communication (WAIC) System request to SC-216 members for feedback on security aspects of upcoming WAIC MOPS document prior to FRAC. A link to document was provided: https://www.rtca.org/sc-236/.
- SC-236 TOR includes: The development of wireless applications must take into account the key issue of spectrum availability, electromagnetic compatibility, and protection. The following aspects should be considered:
  - Protection of spectrum versus this application to ensure the required performances and availability;
  - Protection of other RF users against potential perturbations generated by this application, other users being obviously those which are aircraft embedded but also outside the aircraft; and
  - Protection of aircraft safety systems against unauthorized access (cybersecurity safeguards)
- Hannes Alparslan Continued presentation with way-ahead questions on how to structure document.
- A use case was discussed about airline operations requiring the aircraft to exchange data with the operator's operations center or with other operator services, to serve a wide variety of needs: administrative data transfer (e.g., cabin logbook), flight plan optimization, maintenance support and engine reports, software updates, etc. Currently, most of these use cases are routed on protected spectrum, for historical reasons and airborne architecture constraints. With new generation aircrafts and

engines and with the increased needs from airlines to optimize their operations, the data volume needs are increasing, and congestion issues are now a key concern. It is to be recognized that not all Airline Operations communications have the same performance requirements, which also differ from the ATM ones.

Day 4 – 20 April, 2023

- SG5 DO-DSEC - Data Security- Continued

- Hannes presented assumptions including that data created by the aircraft is trustworthy given the system has been developed in line with appropriate standards
- The objective is to ensure security attributes of data remain at the intended levels throughout the data lifecycle
- Ted Patmore added that the scope ranges from the creation of data to its installation on the A/C onboard server, or the ARINC 645-1 compliant portable data loader.
- Philippe added that data is as trustworthy as its source when it is created. Trustworthiness of the sources is not considered. The standard aims that the security attributes of the data remain adequate for its uses during its all lifecycle.
- The SC-216 /WG-72 group met with SAE S-18/Eurocae WG-63. Discussed interdependencies between Safety and Security. Further leadership coordination meeting between the two groups is planned and will explore opportunities for synergy between the two disciplines.
- Alain recommended that members enroll in the DO-ISEM subgroup

- SG3 DO-392A

- Alain provided a summary of group activity
- SG-3 will need further clarification of scope (Aircraft vs Org) and roles and responsibilities
- DO-ISMS can bridge the gap with respect to risk assessment
- Questions raised about the relevance of customized CVSS

Day 5 – 21 April, 2023

- WG 72 and SC-216 Plenary Day 2, 04-21-2023:

- Cyrille Rosay opened the meeting, and presented the agenda
- Karan reminded everyone that the rules we discussed in Monday's RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, participation and membership policies still apply.
- Subgroups status was provided by subgroups chairs
- Alain provided a summary of the SG-3 activities. The group will setup a working group to review how ED-206/DO-392 should be updated to clarify material.
- Siobvan provided SG4 status: Several presentations were made to help facilitate the development of the ISMS document including presentation from Jean Paul about ICAO. The group determined the volunteers for the subsections.
- Hannes provided SG-5 DSEC status. A proposal for the document structure was discussed with the subgroup. Several questions were discussed including degradation to data security and securing cloud service providers. The group identified document direction, challenge to set objective and a roadmap to reach objective. Hannes highlighted the need to determine specific terms to ensure we all speak the same language. Cyrille suggested that ER-013 should be included in this document.
- Sarah provided a status for SG6. Progress has been made for the development of a change impact analysis guideline.
- A status on coordination with other groups was provided by several members.
  - Siobvan E-36 is in response to the FAA rule that added cyber to propulsion cybersecurity. Propulsion system seem to have similar architecture. Each TC must protect itself.
  - Stefan, G32, We hope to talk w SAE about a roadmap. Stefan has the action to coordinate with SAE to get that presentation scheduled for our June meeting.
  - G34, Siobvan, Group needs to consider cyber per EASA paper . They are trying to create a concept paper to use AI. Cyber is a concern. The group does not want to talk about cyber.
  - SAE S-18/EUROCAE WG-63. Cyrille, Discussed interdependencies between Safety and Security. Further leadership coordination meeting between the two groups is planned and will explore opportunities for synergy between the two disciplines.
- Cyrille offered the 7th floor conf room for next year. All agreed. Cyrille will scheduled next spring meeting in Cologne.

Closing-Adjourn

<u>ACTIONS FROM WG MEETINGS:</u>

- Stefan to formalize actions with SAE S18 to identify and coordinate safety and security processes and WG-72 roadmap with S-18. Need S-18 to talk to us about their roadmap. Need S-18 to consider Cyber per EASA paper. Maybe at June meeting.
- Mitch to develop a presentation on Garmin STS effort relative to change impact analysis
- Sam to develop a list of questions that can be used in a security CIA to help in

assessing security changes. Patrick and Dave to provide input to Sam.

- FAA/EASA to propose a timeline for the “FAQ” document for DO-356B.