RTCA Paper No. 217-23/SC216-145
EUR. 324-23/ WG72-172

St. Denis and Washington DC, 09/22/ 2023

EUROCAE WG-72 Meeting #71 / RTCA SC-216 Meeting #62 Joint Plenary "Aeronautical Systems Security" Meeting Summary	
Date	***Monday – Friday 12-16 June 2023 09:00 – 17:00 EDT / 15:00 – 23:00 CEST***
Place	***RTCA Headquarters (and Virtual)***
Venue	RTCA, Inc, 1850 18th Street NW, Suite 910 Washington, DC 20023
Hosted by	***RTCA***

Attendance:

	Contact	Organisation	June 12	June 13	June 14	June 15	June 16
	Abinash Aryal	Southwest Airlines			X		
	Adam Patrick	Rolls Royce	X	X	X	X	X
	Adrian Waller	Thales Group	X	X	X	X	X
	Alain Combes	Airbus	X	X	X	X	X
	Alan Teyssier	FAA	X		X		
	AmyClaire Brusch	ACI/NA		X			
	Ana Pasuca	IATA	X	X			
	Andrew Drake	NetJets	X	X	X	X	X
	Aneesh Sankruth	Gulfstream		X			
	Anna Guegan	EUROCAE	X	X			X
	Anup Raje	Honeywell	X	X	X	X	X
	Barbara Clark	FAA	X				
	Ben Nagel	CyberBen	X	X	X	X	X
	Brian Petre	GE Aerospace					X
	Bill (William) Trussell	IFR Development	X	X	X	X	X
	Britney Boler	Southwest Airlines			X		
	Carl Schuett	Southwest Airlines			X		
	Cecil Deleon	Southwest Airlines			X		
	Charles Sheehe	NASA	X	X	X		
	Chris MacMullin	Department of National Defence of Canada	X	X	X	X	X
	Cristian Bertoldi	Airbus	X	X	X	X	
	Cyrille Rosay	EASA	X	X	X	X	X
	Dan Diessner	ERAU			X		
	David Chen	FAA	X	X	X	X	

	David Harvie	ERAU	X	X	X	X	X
	David Pierce	GE Aviation	X	X	X	X	X
	Davide Martini	EASA	X	X		X	X
	Deepak Kamath	FAA	X				
	EmersonLuiz Cunha	EMBRAER	X	X	X	X	X
	Esha Vasdev	Department of National Defence of Canada	X	X	X	X	X
	Felix Meier-Hedde	Airbus	X	X	X	X	X
	Filippo Tomasello	EuroUSC Italia					X
	Frédéric Heurtaux	Safran Group	X				X
	Gabriel Elkin	MIT-LL	X	X	X		
	Garv Stephenson	Wisk		X	X	X	X
	Gilles Thales Descargues	Thales Group				X	X
	Hagop Kazarian	Bombardier	X				
	Isaac Lee	Southwest Airlines			X		
	Isidore Venetos	FAA	X	X	X	X	
	J.P. DeKruiff	IOActive Cybersecurity	X				
	Jakub Cunat	Egis Group					X
	Javier Diana	EUROCAE	X				
	Jean-Paul Moreaux	EASA					X
	Jeff Burkey	FAA	X	X	X	X	X
	Johannes vanHoudt	FAA	X	X	X	X	
	John Craig - Shift5	Shift5				X	
	John Flores	FAA	X	X	X	X	X
	John Peace	FAA	X	X	X	X	
	Jose M. Fernandez	Polytechnique	X				
	Jonathan Lee (MIT LL)	MIT LL			X		
	Judicael Gros-Desirs	Airbus	X	X	X		
	Kanwal Reen	Collins Aerospace	X	X	X	X	X
	Karan Hofmann	RTCA	X	X	X	X	X
	Ken Natividad	Southwest Airlines			X		
	Kevin Harnett	IOActive Cybersecurity	X				X
	Kevin Meier	Cessna Aircraft Company	X	X	X	X	X
	Lee Howard	Honeywell	X	X	X	X	X
	Ludovic Donnadieu	Airbus	X		X		
	Luis Lozano	Ineco	X				
	Manon Gaudet	IATA	X				
	Marc Lord	Canda DOD	x	X	x	x	X
	Marcus Labay	FAA		X			X
	Marcus Session	ACI/NA		X			
	Mario Lenitz	Austro Control	X	X		X	
	Mariusz Pyzynski	IATA	X	X	X	X	X
	Mark Hingsbergen	GE Aerospace	X				
	Mark Kelley	Belcan	X	X	X	X	X
	Marshall Gladding	Boeing		X	X	X	X
	Marty Reynolds	A4A	X				
	Matthieu Willm	Dassault Aviation	X	X	X	X	X

	Michael Vanguardia	Boeing					X
	Michael Welch	FAA	X		X		
	Mikaëla Ngamboé	Polytechnique	X	X	X	X	X
	Mike McCartney	FAA		X	X		
	Mike Noorman	GE Aerospace					X
	Mike Shalvey	Southwest Airlines			X		
	Mike Tumminelli	Gulfstream	X	X	X	X	X
	Mila Obradovic	Canada DOD				X	
	Milton Santos	EMBRAER				X	X
	Mitch Trope	Garmin	X	X	X	X	X
	Nicolas Durandeau	EASA	X		X	X	X
	Nikita Johnson	Rolls Royce	X	X	X	X	X
	Olivia Stella	SWA	X	X	X	X	X
	Pamela Davis	Southwest Airlines			X		
	Patrick Morrissey	Collins Aerospace	X	X	X	X	X
	Peter Tsagaris	TCCA					X
	Phil Watson	Panasonic	X	X	X	X	X
	Phil Windust	FAA	X	X	X	X	X
	Philippe Dejean	Safran Group	X				X
	Prachi Shekhar	EGIS Group	X	X			
	Pieter Wessel	Canada DOD			X	X	X
	Rob Hood	Astronautics			X	X	X
	Romuald Salgues	Airbus Helicopter	X	X	X	X	X
	Rosemberg Andre da Silva	ANAC-Brazil	X			X	X
	Sam Masri	Honeywell	X	X	X	X	X
	Sarah Stern	Boeing	X	X	X	X	X
	Seth Stewart (PWC)	PRATTWHITNEY			X		
	Siobvan Nyikos	Boeing	X	X	X	X	X
	Stefan Schwindt	GE Aerospace	X	X	X	X	X
	Stephen Van Trees	FAA	X				
	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
	Tim Stelkens-Kobsch	DLR	X				X
	Varun Khanna	FAA	X	X	X	X	X

Day 1 – 12 June, 2023

- WG 72 and SC-216 Plenary Day 1, 06-12-2023:

- Patrick M. and Siobvan N. opened the meeting, greeted participants
- Karan Hofmann and Anna Guegan presented the RTCA and EUROCAE plenary meeting mandatory slides including the RTCA and EUROCAE anti-trust, IPR, GDPR, participation and membership policies.
- Siobvan N. presented the agenda and facilitated introductions of participants around the room and online.
- Minutes from April meeting will be posted during the week and their formal approval is scheduled for Friday.

- Regulatory Update:

- Davide Martini presented EASA regulatory update:
  - Davide discussed Part IS Implementation journey. AMC/GM will be published by end of July 2023. Changes right now are only adding clarifications to existing information. Next steps before publication are formal checks, proofreading and executive director's decision which should take approximately 4 weeks. All orgs should be compliant by end of 2025. Two years will allow orgs to get familiar so they can be compliant on time. Pilot program will provide a reality check.
  - EU design approval applies for products under ETSO.
  - Matthieu W. asked about applicability of part IS for the FAA. Varun K. responded that at this point Part-IS is not applicable in the US and that the FAA has not mandated anything yet. The concern with Part-IS is that the US industry was not involved in its development. At some point it will be renegotiated with FAA.
  - Davide - The proposed Part-IS regulation does not apply to organizations currently covered by a Safety Agreement signed between their country and the EU. However, this does not preclude the possibility for a future re-negotiation of those Safety Agreements in order to include certain provisions related to the management of information security risks.
  - It is important to note that even if those third-country organizations are not subject to the requirements of the proposed rule, this does not preclude that the persons or organizations in Europe that are subject to this rule may impose certain contractual requirements when buying those products from the third-country organizations.
  - EU organizations will have to address information security risks coming from the interfaces they have with other organizations or because of the products they use.
  - It must be noted that these are organizational requirements, not product certification requirements. Therefore, the question is about the risks coming from the third-country organization if it is not managed appropriately.
  - This impacts the product (e.g. not properly addressing in-service experience, not having sufficient staff to address information security risks at organizational level, etc.).
  - The oversight of the EU organizations subject to the rules will be performed by the EU Member State competent authority or, if applicable, by EASA. As part of this oversight, the competent authority will check how the organization manages the risks coming from their suppliers.
  - Davide - There is a specific case with MRO's : An MRO maintaining EU registered aircraft requires an EASA Part 145 approval and Part-IS applies. For a US MRO with an EASA Part 145 approval obtained through the BASA, Part-IS doesn't- apply, hence a regulatory discrepancy for MRO maintaining the same aircrafts.
- 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.
  - Rulemaking effort completed, currently working on second go on the rulemaking,

making some updates, talking about ICAs now, adding teeth into the ICA requirements, it is harmonized, after September it will go to legal, it should go for public comments by November-December. The new rule covers parts 25, 33, 35. Content will be similar to EASA's 1319 rule. Similar to the special conditions today. The AC will not go into details. It will invoke the RTCA docs.
    - Philip W. added that FAA is not developing an equivalent to EASA's part IS. FAA has to coordinate with TSA on Cyber.
    - Advanced Air Mobility has conflict between TSA and FAA.

- HICLASS project in the UK on Common Modes guidance for DO-356A/ED-203A By Adrian Waller/Thales UK:

- Adrian introduced the "High-Integrity, Complex, Large, Software and Electronic Systems" (HICLASS) project.
- The HICLASS project is supported by a joint UK Government and industry investment to maintain and grow the UK's position in civil aerospace design and manufacturing.
- HICLASS goal is to drive new technologies and best-practice throughout the UK aerospace supply chain.
- Part of HICLASS work was to analyze aerospace security standards for the purpose of identifying maturity gaps within the standards and sharing best practice of security objective conformance.
- A white paper (Report) was written to provide guidelines and considerations around ED-203A/DO-356A Security Refutation Objectives. The report focusses on how to plan for security refutation test activities, and considerations in order to meet the Security Refutation Objectives.
- The report provides additional guidance for vulnerability scanning, the interpretation and triage of the results and scoring vulnerabilities for airborne systems as well as further guidance on security measure common mode analysis.
- Diversity should not be applied for its own sake. A number of key program level considerations regarding Diversity should be made and traded off against the System or Item, such as cost, time, practicality, complexity, level of risk, etc.
- The very application of Diversity in a number of areas will, potentially, increase the level of risk, have other negative impacts, or have benefits that are hard to quantify
- It is in general costly, difficult and counterproductive from a security point of view to attempt to eliminate shared security infrastructure (e.g. by producing multiple redundant key management systems). Best practice is to develop one, well designed and highly assured, security infrastructure.
- The report is available at: https://www.adacore.com/uploads/techPapers/Guidelines-around-ED203A-and-DO356A-Security-Refutation-Objectives.pdf

- Companion FAQ document to DO-356A/ED-203A – intro by Nicolas Durandeau/EASA

- Nicolas presented seven potential topics to be considered for the FAQ document including SAL assignment for potentially Catastrophic and Hazardous threat conditions, the use of COTS for security measures, the use of operational security measures, defense in depth concept, security risk assessment methodology, and the clarification of threat scenarios and their security attribute and associated security measures.

- Alignment with IAQG Supply Chain Management Handbook (SCMH) By Stefan S. and Gerald L. (Gerald L. was unable to attend)

- Stefan mentioned the IAQG SUPPLY CHAIN MANAGEMENT HANDBOOK -SCMH. The handbook is geared towards manufacturing. It attempts to provides help for protecting business ops ransomware. SCMH sections are structured around standard supply chain processes. It is looking to solve all cyber issues including safety and business.
- Nikita Johnson- Supply Chain is probably the area of ISMS that has the most overlap/conflict with national security requirements. There have been discussions on

how to resolve some of these conflicts across different regions/countries.

- Crypto agility (hardening of air/ground signals)

- There was a discussion on rules about security backward compatibility and the ability to sunset prior crypto scheme in shorter than the standard 6 years. What is the rule for legacy avionics, in the transition period,
- Agility, Certification burden and the ability to update cryptographic schemes. Is the update treated as a minor or major change? This subject will remain open for now and will be discussed at a later time.

- E-36 & SAE AIR 7368 By Mark Hingsbergen and Deepak Kamath

- A presentation was given providing E-36 & AIR 7368 report. Document #1/21/21 is almost ready for publication.
- This document is to provide guidance for aircraft engine and propeller systems cyber security certification. This document is planned to serve as a replacement for propulsion issue paper.
- Discussion on having the engine distrust the rest of the a/c for cyber…Big industry, hard to establish trust, but the more we are aware of what others are doing the better we can perform our cyber sec.
- Matthieu Willm: We need to keep in mind the assumptions of the risk assessments, such as excluding state level attackers or assuming that maintenance personnel are not malicious, etc.
- It was noted that SAE Air documents are used as industry information documents and are not typically used as MOPS documents. Info for engine may need to be added to DO-356 document.

- SG 4: ISMS part 1 Scope level set

- Siobvan N. presented slides on the scope of the ISMS document.
- Mike Tumminelli added that in operational technology. when you talk of product security, you refer to both physical and cyber security even though physical security and information security are not typically part of the same organization in companies.
- Ben N.. added that there will be small or young companies that might develop a fully integrated (Safety, Security and Information Security) management system, and some that will have a set of multiple management systems. There needs to be a link between these domains.
- Mike Tumminelli asked if we can classify suppliers by what SAL/DAL system they supply and demand different security standards/levels?

End of day one

- WG 72 and SC-216 WG Meetings - Day 2, 06-13-2023:

- SG4 ISMS Information Security Management System continued-

- Patrick- shared agenda - We will continue ISMS discussion
- Davide Martini presented EASA's insight from AMC and GM comments to Part-IS. The majority of the comments were related to the Risk Assessment, ISMS, and incidents reporting requirements.

- Airport perspective/considerations

- From Airport perspective, AmyClaire Brusch from Airport Council International/North America thanked the group for inviting airports to the meeting. AmyClaire introduced Marcus S.
- Marcus S explained that using NIST framework, airports have to meet other regulations that come up every year, including PCI etc. TSA reporting is another. Requirements might be too broad. The effect of these requirements is too grave. Different entities telling airports to do things differently. So much oversight making airports less safe. Trying to comply with so many regulations is all we are able to do because it is taking so much time. Smaller airport have less funding to do what is needed. Collaboration with groups like RTCA will help to make solutions that are collaborative. Marcus added that it is good idea to be part of this group making standards,
- AmyClaire added that time is needed to comply and it is very costly. For example audits can be very expensive. Smaller to medium airports can not afford compliance to the regulations. Complexity of the aviation echo system contributes to the problem.
- Siobvan N. agreed and welcomed AmyClaire and Marcus participation and wished for participation of smaller airports in writing the ISMS document. Siobvan suggested to work through ACI (Airports Council International – North America) to participate with RTCA and EUROCAE.
- Stefan provided a summary of part IS to make sure airports are aware of what is becoming a new requirements in Europe.
- AmyClaire added that part of the challenges for airports include interfaces between the airport and the operators (airlines), responsibilities for airport ops and the fact that there is no commonality between airports. Some airport systems that are not associated with airlines maybe impacted. Marcus added that these General Aviation airports are in scope but not getting the same oversight, different airports have different models.
- Garv Stephenson asked if DO-230, Airport Security Access Control Systems, is being widely implemented at smaller airports, air fields, heliports, & vertiports. Marcus responded that it is not widely. There is no regulatory entity enforcing regulations.
- Karan H. pointed out that DO-230 is only offered as a guideline and thus usually is not enforced. Marcus added that small airports may not be able to do what DO-230 is asking for.
- AmyClaire added that smaller airports are learning and providing valuable feedback about what would be hard for them to comply with. Marcus added that small airports should be engaged in the conversation through different channels. .
- Siobvan added that info necessary for airports to join SC-216 subgroups and participate will be provided.

- Update to Distance to Aircraft Presentation by Matthieu Willm

- Matthieu discussed accounting for distance to the aircraft in risk assessments. Matthieu discussed the number of hops to safety effect and the effectiveness of the security measures at each hop.
- Felix Meier-Hedde suggested that then we should plan for a chapter on safety impact and address safety effect of hops as we perform security risk assessments.
- Matthieu added that we need to establish a link between IT security and product security to help identify safety impact
- Matthieu added that he advocates for performing a single risk assessment for each

security domain that provides substantiation that it can handle safety risks up to a predefined level.

- Stefan Schwindt added that we have a subgroup for risk assessment to incorporate this material. He said that this will probably be an original write up section, as we should be able to borrow from standards such as ISO 27001/27002, 62443, etc for other sections.
- Alain Combes said that when discussing about whether one asset is Part IS related or not (like Nav DB) we should not only be considering the approved organization applicability but also the risk to an interface to a Part IS impacted organization

- ISMS parallel with safety presentation by Sam Masri

- Sam Masri discussed the similarity between SMS and an ISMS program.

- Walkthrough of ISMS topics/subgroups

- Felix presented an outline of a white paper being worked on discussing ISMS and ISEM. It included sections on ISEM Org, policies, methods and tools among many other topics.
- John Flores asked if there is a proposed training curriculum specific to ISMS, Part IS that can be proposed to narrow and specify the type of training being suggested.
- Garv Stephenson responded that we could potentially leverage the NIST CSF (cybersecurity framework) for ISMS assessment and assessment training
- Garv Stephenson provided the link: https://www.nist.gov/cyberframework
- Stefan Schwindt added that we should take the SMS approach of giving objectives of identifying and ensuring competence of staff
- Cyrille added that you can check the status on SMS regulation at EASA using the link: https://www.easa.europa.eu/en/domains/safety-management/safety-management-system/sms-easa-rules#atmans
- Ted Patmore provided a link to SMS Summary: https://eurocae.sharepoint.com/:w:/r/sites/strato/34fd374d-a1c8-e811-8154-e0071b66a0a1/d07cc886-a856-ed11-bba2-000d3adea767/Additional%20input/Pillars_of_SMS.docx?d=w7db51a875bdf423b9442ae0801df2956&csf=1&web=1
- Felix added that most organizations will have an ISMS in place for business reasons. The effort to consider safety risk in addition to business risk should not be that big.
- Cyrille provided a link to the FAA SMS: https://www.faa.gov/about/initiatives/sms/specifics_by_aviation_industry_type
- Felix added that we should distinguish primary assets (with safety effect) from supporting assets that expose primary assets to security threats.
- Chris M. agreed and added that the process we use reduces assets to what we call "cyber assets". From there we do attack path analysis. and evaluate the chains that lead to these critical assets. He added that this method, however, is from the context of the aircraft boundary.
- Stefan Schwindt presented an approach for developing an ISMS using ISO material.
- Siobvan commented that the approach is good however not everyone in RTCA or EUROCAE has the ISO membership and login to get ISO docs
- Thomas Parmer suggested that NIST is open for all

- Supply Chain Security By Adam Patrick and Mike T.

- Adam and Mike presented a chart on security across supply chain and supplier management and interaction. They also discussed strategies for sharing risks across the supply chain.
- Cyrille added that ED-201A external agreements may also provide some element to be considered when it comes to the sharing of risk. EASA and FAA can also share audit results. This would mitigate the potential for extra audits
- Cyrille pointed to resources that could be helpful in the supply chain subject such as AIA Supply Chain Report, NIST SP800-161, NIST SP800-218 and ISO27000 Series.
- Phil Watson added that US DoD requires CMMC for supplier security and provided the link: https://dodcio.defense.gov/CMMC/

End of Day 2

- WG 72 and SC-216 WG Meetings - Day 3, 06-14-2023:

- Vulnerability Management / ED-206 impacts based on the UK HICLASS By Nikita Johnson

- Nikita Johnson presented a PCS Best Practice Guide for Vulnerability Management presentation.
- The guidance focus was to augment ED-202A/ED-203A and ED-206.
- The guidance topics included Refutation testing, vulnerability management, and Change impact Analysis
- We have parallel between safety and cyber sec reporting. We may have to handle it differently. Conflicting reporting is a challenge that need to be dealt with. Types of things you might report depending on what vulnerabilities you find. Timing variabilities in availability of an aircraft for forensic analysis is another issue.
- Some of the vulnerabilities may change and then you have to look at the architecture to see how they would affect the system.
- Reporting is required when the vulnerability could rise to a CAT or HAZ effect and certain major conditions.

- CSDS Paper & Feedback from SG3 By David Harvie/Embry-Riddle

- David presented a draft joint AIA/US ACCESS paper on ED-206/DO-392. The presentation discussed security risk management, information sharing, security events detection strategy, and gave an overview of cybersecurity data science in context of aviation.

- CSDS uses cases on factory/OT, airports, etc. By Gabe Elkin/MIT

- Gabe provided a presentation on CSDC research purpose and planned products. CSDS research was performed to accelerate aviation industry timely adoption of novel CSDS and AI/ML technologies for the enhancement of cybersecurity for the airlines, airports, and aircraft elements of the national aviation ecosystem to increase safety and resilience.
- Study looked at airlines, airports and aircrafts and explored using automated data analysis help in addressing vulnerability exploitation likelihood
- Carl Schuett asked if the model can be trained to see what normal looks like so that any abnormal behavior can be identified. That seems like an approach that would be needed in conjunction with training the model to see specific attack types.

- Honeywell risk management policy overview By Anup Raj/Honeywell

- Anup gave a presentation on risk management at Honeywell.
- Garv S. provided a link for NREL guidance on Addressing Electric Aviation Infrastructure Cybersecurity Implementation: https://www.nrel.gov/docs/fy23osti/82856.pdf
- Siobvan N reminded the group that ISEM FRAC completion is planned for September 2024. She added that we can get started by collecting the data that we currently have.
- Cyrille Rosay asked to please consider ED-206 appendix C (vulnerability scoring) as there are already notions in it (on aircraft vs off aircraft) that may need to be reworked and refined. Cyrille recommended to start from this annex.
- Cyrille provided a link for the French Cyber Security agency CVSS scoring for ICS: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf. He added that we can potentially tailor this for scoring.

End of day3

- WG 72 and SC-216 WG Meetings - Day 4, 06-15-2023:

- Southwest Airlines Safety Management System and Change Impact Analysis By Olivia Stella and Tara Knight

- Olivia gave an overview presentation on the Southwest Airlines Safety Management System and Change Impact Analysis.
- Olivia said that SW Airlines approach for managing risk and assuring safety risk controls is based on 4 components that include a safety policy, a safety risk management system, performance measurement and safety communication, promotion and training.
- Olivia also gave an overview of the CIA process at SW by showing a workflow diagram. The process emphasizes business impact and effective risk control.
- Stefan added that Managing changes through the ISMS is a topic that needs to be added (from operational/procedural point of view).
- Sarah added that we should look at the full life cycle of the product. For example, for a data loader, looking at the integrity of the downloads that is provided to the OEM would be needed
- Siobvan added that for operator we do need to capture the different parts for the lifecycle of the product . (operator, back office, secure data loader, maintenance, sec logs, diversity and handling of the logs) …security logs capture - arinc 645 is defining security for the data loader.
- Cyrille presented 2 charts on determining the level of threat effectiveness of the security protection and how long a system stays secure.
- Sam Masri reminded participants to review April meeting minutes that were posted at: https://aeropus.i3cloudservices.com/Group/GroupLanding/53?tab=Documents&folder=2023+Meetings%2F1-April+17-21%2C+2023+-+61. He added that he will be asking for approval of minutes during day 5 plenary meeting.

- SG-6: DO-326/ED-202 Change Impact Analysis By Sarah and Stefan

- Sam Masri reviewed CIA questions and noted discussed updates.
- Chris MacMullin asked how these questions are relate to 356A. An example of their use is found in Table D-1 of section D.2.2.1.3
- Stefan Schwindtresponded that it is in the common risk assessment appendix
- Chris MacMullin confirmed that Section 3.1.1.1 in 356A provides Asset Identification Considerations
- Nikita Johnson added that there maybe some overlap with the "hops from safety impact" discussion from Monday as a consideration for change
- Stefan Schwindt agrees and added that we should reflect upon the considerations in DO356A for our change impact analysis. He said, DO356A is really a "clean sheet" risk assessment. Our CIA is a "delta risk assessment" so they can't be worlds apart. However, we want to move away from saying we need to have or establish a full DO356A analysis for every change
- Lee H. expressed interest in a security CIA for a propeller
- Stefan Schwindt added that because it is, for example, a mechanical change, we don't need a DO356A analysis to be able to say that there is no risk
- Matthieu W. added that physical changes can impact security, for instance making a digital interface that was deeply buried and needed hours of dismantling to be accessible
- Stefan S. agreed and added that this is why all changes need to consider security and not simple statements that mechanical changes are not security. Hence "affected areas"
- Rob Hood added that his company performs a COTS/OS detailed CVE analysis and report any CVEs as exploitable and recommend patching. However, that same Aircraft/product could have hackable protocols that are being used in an external interfacing network. External facing networks with direct safety impacts and glaring exploitable weaknesses are a real concern. He added that he is not aware of any mechanism requiring ongoing risk assessments (except in the initial or recurring STC).

Regarding STC, Rob asked that if an OEM uses WPA (or even WPA2) for 10 years and proposes an STC to add a new external network connection. Should there be a review of the old WPA?

- Chris MacMullin asked if the point of the question is to determine if there is a need do "more" based on the determination of potential impact (maybe vulnerability exposure)? He then added that if so, then the follow-on would be a conversation about initiating a risk assessment or a trigger for an update to an existing risk assessment. This would be either within the system being evaluated or rolled up to the higher order system/platform.

- SG-5- Security lifecycle presentation By Kanwal

- Kanwal presented data flow charts for a typical product lifecycle, SW part end to end distribution and a common security method for SW distribution. She also gave an overview of a typical field loadable software signed electronic distribution process.
- Installation part can be added to lifecycle – SW will be transferred by different media. Use case is limited to airborne SW. Process of loading may have separate treatments. Where do we want to see the signature being attached. Where is the human in the loop.
- Garv Stephenson added that Fig 2-1 in DO-355A also has a life cycle diagram like this. He also recommended to look at ARINC 835-1 Figure 5-1 for additional detail on SW distribution to aircraft, although it is Boeing centric. For data logs life cycle Garv recommended looking at ARINC 852 figure 6-1.
- Stefan Schwindt agreed that it is a good source to try to ensure we create a good generic lifecycle
- Olivia Stella added that a part that's missing in the life cycle is disposal and decommissioning
- The group discussed potentially starting the draft of this section in order to move the document along and get feedback from the larger group.

- Security Dataflow Diagrams By Patrick M.

- Patrick Morrissey presented several Data Flow Diagram (DFD) models . One of the models included availability, integrity and confidentiality. He also presented several threat models.
- Stefan Schwindt added that ASTM standard uses DFD for risk modeling
- Cyrille Rosay pointed to the Bi-Directional threat model presented on page 157 in the ARAC report: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf
- Phil W added that DataLoaders should not be trusted; rather, there should be a requirement for digital signatures on all loads to verify authenticity & integrity.
- Stefan Schwindt added that for the DFD, trust may be relative and you would need to justify the boundaries. They can be different forms of security measures (such as signature check). Some data maybe a pass through data. You want to show data flow. You want to show digital and logical flow. Consider bidirectional or unidirectional connections. Look at your configuration and programming or re-programming, if it can be manipulated maliciously . How do you link this to model based engineering.
- Ted Kalthoff provided a link for a Microsoft threat modelling tool. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- Mitch Trope provided a link for a recommended threat modelling book:
- Adam Shostack's book on threat modeling: https://shostack.org/books/threat-modeling-book
- Olivia Stella added that OWASP has their own open source threat modeling tool that generates a model and a sequence diagram: https://owasp.org/www-project-threat-dragon/
- Olivia also provided the link: https://owasp.org/www-project-pytm/ and another link for an article that references 4 different threat modeling tools https://michenriksen.com/blog/drawio-for-threat-modeling/

- Garmin STCs By Mitch T.

- Mitch T. provided a high level overview of Garmin STC process. He provided several Part 23 and Part 25 STC examples. He also discussed approving and fielding changes. He discussed Change Impact Analysis for Part 25 STC.
- Agreements have to be in place to process proprietary data in an STC.
- Manuals stay with the ac. New owner responsibility is to review that. Also review all the ADs for the a/c. You can do field approvals on part 25 a/c. you still need enough data to be able to get it approved.
- Part 25 rules are different from part 23. You still need enough data for the change.

End of Day 4

- **Day 5 – 21 June, 2023**

- WG 72 and SC-216 Plenary Meetings - Day 5, 06-16-2023:

- Karan, started the meeting with SC-216 awards. Formal award presentation is scheduled during the 2023 annual RTCA meeting.
- Varun, Mitch, Pat, Dave and Sam were presented with RTCA awards for their work on DO-392. While Varun and Siobvan were presented with RTCA awards for their work on DO-393.
- Minutes from April meeting were approved
- WG 72 and SC-216 Plenary Meetings schedule was presented
- Dec 4th week meeting is planned to be hosted by **Honeywell, Deer Valley facility at 21111 N 19th Ave. Phoenix Arizona**.
- April 2024 meeting is planned to be hosted by EASA in Cologne Germany.
- FAQ doc will need a timeline. There are only 7 FAQ topics. Varun and Siobvan have many topics. May need to put it off until enough topics can be covered.
- Karan H noted that RTCA may not require FRAC for an Interpretations of guidance material document - could be a white paper. However, it needs to be added to the TOR
- Stefan suggested that we should go through FRAC. Varun agreed and added that industry input would be helpful.
- This may be equivalent to NAC in Europe. Anna asked if it is going to be provided for Free or for a cost.
- Stefan added that we have many FAQ documents out and should follow the same method. It can be similar to ED-94C/DO-248C.
- Ben Nagel will be a focal for the committee to collect topics for FAQ.
- Action to everyone interested to provide topics to Ben Nagel.
- Stefan suggested that we maybe able to start on the FAQ doc by mid 2024.
- Resources maybe limited- may need to visit this FAQ in DEC.
- Stefan alerted participants to ensure no proprietary info is included in FAQ topics proposal
- There were questions Nicolas/EASA on the COTS presentation to. Nicolas confirmed that it is possible to take credit for work done for cots - for example test coverage- However, you need to show you don't have unknown functionality. Should look at context and protection profile. Show the area that is not covered and show the same objective. ED-305 provided a position when using cots. You may use a protection profile against the COTS component. COTS doesn't get a free pass. Should bring evidence in-how do you show correct mapping. Your protection profile maybe different. Use architecture to mitigate COTS failure. Nicolas asked that participants can send him questions related to COTS directly.
- Jean Paul provided a status from ICAO. One paper presented by the US about how to collaborate material-two WGs technical-talk about security management and another about info sharing and another about incident response- looking at what EUROCAE has done in that subject-with respect to ISMS, an interesting work on a menu explaining objective- potential for overlap- Jean Paul will coordinate between panels including ARINC-agreement on security objectives-kickoff of ad hoc cyber sec committees, coordinate between ICAO and standards committees-2 panels- one on isms and another on -global regulatory work at ICAO-identify systemic issues where new rules are required-

- Subgroup status:

- Subgroups status was provided by subgroups chairs. The groups presented a summary of progress made and remaining issues to clear path forward.

SG3-

- The group will be working on the interface with the ISMS document as well as aligning different vulnerability scoring models with different objectives.

SG4-

- The group will be working to make sure ACI and airports join SC-216 and SG-4 ISMS.
- A chapter leader and subgroups will be setup
- Risk management group is to identify number of risk levels for security controls subgroup and SG-3.
- Safety integration subgroup to consider changes to ISMS
- Start editorial work- need to be published in July for EASA.
- Per Jean Paul US paper is considering ISMS-we want the standard to be used by authority and industry.

SG-5

- The group will be working on first draft and a use case for September
- Olivia will lead SG-5
- There will be a SG leadership meeting to discuss moving forward plan.

SG-6

- The group will continue work on the CIA
- Group members to provide examples for testing CIA guidance
- The group will be working on a proposal for ED-202A/DO-326A and ED-203A/DO-356A alignment
- Varun noted that Congress is dictating that any change to a catastrophic or Hazardous system is a major/significant change. Stefan added that this is also EASA's position. This issue may cause a heartburn with industry and can increase workload- EASA's guide is in 21.A.91.(GM.21.A.91)
- Nikita Johnson added that there was quite a lot of discussions around change to cyber 'legacy' systems and the risk assessments associated with them. These discussions happened during the SG6 WG meetings when reviewing the proposed CIA questions.

- Coordination with other groups:

ICAO-Stefan

- ICAO Communications panel is working on developing several documents addressing PKI policy, Security Risk Assessments, IPS Security.
- ICAO Trust Framework Panel is developing an ISMS for aero communication document
- ICAO Cybersecurity Panel is working on several documents addressing Cyber threats and risks, and providing cyber guidance material

SAE-Siobvan

- SAE G-32 has an open ballot until July 2023 for JA6678 document
- SAE E-36 is working on AIR 7368 Standard for Propulsion Cybersecurity. The group has Ballot 3 and comment log posted
- SAE G-34/WG-114 AI/ML in Aviation committee should consider cyber security per EASA AI concept paper

RTCA-Siobvan/Stefan

- DO-404 / ED-315 FRAC ended May 19
- June 12-16 SC-223 / WG-108 Plenary
- DO-379A / ED-262A in development, working towards FRAC
- A858 Part 1 Supplement 1, Part 2 Supplement 2, & Part 3 planned for release in 2024
- WAIC committee integrating feedback received from SC-216. On track to finish in 2023.

ARINC-Siobvan

- Next ARINC NIS AEEC meetings scheduled for June 12-14 in Milwaukee, WI (A811 and A822)
- ARINC 827, 835, 645-1 are being reworked (SW security, secure data loading related)

S-18/WG-63-Siobvan

- ARP4754B, document is in final review before release. Expected publication June 2023
- ARP4761A, Document is in final review before release. Expected publication June 2023
- AIR6276, Draft document review planned for the 2023 Q2 plenary. Planned ballot during 2023 Q3

- AIR6913, Draft document review planned for 2023 Q2 plenary. Planned committee ballot during 2023 Q4
- AIR7126, Common Cause Errors (CCE) is still in initial stages.
- AIR7121, Applicability of Existing Development Assurance and System Safety Practices to Emerging Technology Products. A draft for general review is planned for Q2 2023.
- AIR7127, Human Considerations for Functional Hazard Assessments is still in initial stages.

Other Cyber Related Standards-Siobvan

- International Aerospace Software Quality industry standard (AS 9125) for the effective control of non-deliverable software is being updated
- IAQG Supply Chain Management handbook is being updated
- ATA Spec 42 is being updated. Spec 42 provides recommendations on standardized methods to achieve the appropriate level of security for an application primarily relying on digital identities.

ECSCG & US ACCESS WG-Cyrille

- European Cybersecurity Standards Coordination Group (ECSCG)- Current Cybersecurity Rolling Development Plan is posted at https://ecscg.eu/media/1249/ecscg-c-rdp-v40.pdf
- US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS)- Next meeting July 12

A-ISAC-Kanwal

- 2Q AvTech June 21-22 at United in Chicago
- Aviation Cybersecurity Summit week of September 11 in Dublin

FAA-EASA Safety Conference-Cyrille

- FAA focus on addressing cyber risks that could potentially impact product safety
- FAA is committed to working closely with EASA
- FAA will not issue a regulation addressing organizations similar to Part-IS
- Addressing Part-IS in the BASA will be challenging. However, both Parties stated that they will do their best to avoid having Special Conditions in place.
- FAA is committed to closely work with EASA to facilitate this process.

New business- none

END 1231PM

ACTIONS FROM WG MEETINGS:

- Action to everyone interested to provide potential FAQ topics to Ben Nagel
- FAA/EASA to propose a timeline for the “FAQ” document.
- 2024 September meeting location may have to be changed away from Paris because of the Olympic Games. Cyrille will look into a new location.
- Siobvan to provide info necessary for airports (AmyClaire and Marcus) to join SC-216 subgroups and participate.
- Sam M took the action to add the Training subject to the safety section for the ISMS.