RTCA Paper No. 309-23/SC216-147
EUR. EUR 350-23/WG72-92

St. Denis and Washington DC, 12/07/ 2023**

EUROCAE WG-72 Meeting #72 / RTCA SC-216 Meeting #63 Joint Plenary
“Aeronautical Systems Security” Calling Notice

Date	***Monday – Thursday 18-21 September 2023*** *09:00 – 17:00 CEST / 03:00 – 11:00 EDT* ***Friday 22 September 2023*** *09:00 – 13:00 CEST / 03:00 – 07:00 EDT*
Place	***EUROCAE Headquarters (and Virtual)***
Venue	EUROCAE: 4th floor 9 rue Paul Lafargue 93200 Saint Denis – France
Hosted by	***EASA***

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

	Contact	Organisation	April 17	April 18	April 19	April 20	April 21
	Adam Patrick	Rolls Royce	P	P	P	P	P
	Adrian Waller	Thales Group	X			X	X
	Alain Combes	Airbus	P	P	P	P	P
	Alex Milns	EUROCAE	X	X	X	X	X
	Ana Pasuca	IATA	X				X
	Andrew Drake	NetJets			X	X	X
	Anna Guegan	EUROCAE					X
	Anup Raje	Honeywell	X	X	X	X	X
	Ben Nagel	CyberBen	P	P	P	X	X
	Bernard Margelin	Airbus			X		
	Bill (William) Trussell	IFR Development	X	X	X	X	X
	Borja Garcia-Blanco Castro	EASA	X				
	Cyrille Rosay	EASA	P	P	P	P	P
	Dan Diessner	ERAU	P	P	P	P	P
	Daniel Locke	CORASSURE		X			
	David Harvie	ERAU		X	X	X	X
	David Pierce	GE Aerospace	X	X	X		
	Davide Martini	EASA		X	X		
	Emerson Luiz Cunha	EMBRAER	X	X	X	X	X
	Felix Meier-Hedde	Airbus		X	X	X	
	Garv Stephenson	Wisk	X	X	X	X	
	Gilles Thales Descargues	Thales Group	X	X	X		X
	Hannes Alparslan	European Defense Agency (EDA)	X			X	
	Harry Wingo	US ACCESS					X
	Isidore Venetos	FAA	X			X	
	Javier Diana Lopez	EUROCAE	P	P	P	P	X

	Jean-Paul Moreaux	EASA			X		
	Jeff Burkey	FAA	X	X	X	X	X
	John Flores	FAA	X	X	X	X	X
	John Peace	FAA	X			X	
	Jose Romero-Mariona	Raytheon Technologies	P	P	P	P	P
	Jonathan Lee	MIT - Lincoln Labs				X	
	Kanwal Reen	Collins Aerospace	P	P	P	P	P
	Karan Hofmann	RTCA	X				X
	Kathleen Finke	Astronautics				X	
	Ken Kitamura	JCAB	X	X	X	X	X
	Kevin Meier	Cessna Aircraft Company	X	X	X	X	X
	Kristof Lamont	EuroControl					X
	Laurent Leonardon	Collins Aerospace	P	P	P	P	P
	Lawrence Baker	NCC Group			X		
	Lee Howard	Honeywell	X	X	X	X	X
	Levi Jones	CORASSURE	X	X			
	Manon Gaudet	IATA			X	X	
	Marcos Ramos	Embraer	X	X	X	X	X
	Mariusz Pyzynski	IATA	X	X	X		
	Mark Kelley	Belcan	P	P	P	P	P
	Marshall Gladding	Boeing	P	P	P	P	P
	Matthieu Willm	Dassault Aviation	P	P	P	P	P
	Michael Welch	FAA				X	
	Mickael Sabelle	Collins Aerospace					X
	Mikaëla Ngamboé	Polytechnique	X	X		X	
	Mike Tumminelli	Gulfstream	X	X	X	X	X
	Mila Obradovic	ECN		X	X	X	
	Minh Trang	Airbus			X		
	Mitch Trope	Garmin	P	P	P	P	P
	Nha Nguyen	Boeing	X				
	Nicolas Durandeau	EASA	X	X	X		X
	Olivia Stella	SWA	P	P	P	P	X
	Patrick Morrissey	Collins Aerospace	P	P	P	P	P
	Phil Watson	Panasonic	P	P	P	P	P
	Philippe Dejean	Safran Group	P				P
	Prachi Shekhar	EGIS Group		X	X		
	Raphael Blaize	Thales Group	X	X			
	Rosemberg Andre da Silva	ANAC-Brazil	P	P	P	P	P
	Sam Masri	Honeywell	P	P	P	P	P
	Sarah Stern	Boeing	X	X	X	X	
	Siobvan Nyikos	Boeing	P	P	P	P	P
	Stefan Schwindt	GE Aerospace	P	P	P	P	P
	Tara Knight	SWA	X	X	X		
	Ted Kalthoff	Archer Aviation	X		X	X	X
	Ted Patmore	Delta	X	X	X	X	X
	Thomas Parmer	FAA	X	X	X	X	
	Varun Khanna	FAA	X	X	X	X	X
	Vic Patel	FAA	X	X	X	X	
	Vitaly Guzhva	ERAU				X	
	Will Stephenson	MIT - Lincoln Labs				X	
	William Yu	Volant Aerotech	X	X		X	

**Post Meeting Note: The date at the top of the meeting minutes reflects the last date it was revised, not the date that the meetings occurred.

Day 1 – 18 September, 2023

- WG 72 and SC-216 Plenary Day 1, 09-18-2023:

First introductions by Javier as he is filling in for Anna
Karan introduced herself as well

- RTCA Anti-Trust
- RTCA Proprietary Slide
- RTCA Committee Participation Membership Policy

Javier went through some of the EUROCAE slides

- EUROCAE IPR Policy
- GDPR and Privacy

Karan wanted to go over new RTCA Security Courses
RTCA and EUROCAE are co-hosting an Aviation Summit for Future Connectivity

- Virtual
- October 25th

Javier went over EUROCAE Facility heads up
No questions from the committee

Introductions through Siobvan

Sam asked about minutes so we can review and approve on Friday

Regulatory Update

- Varun
    - Rule making is still underway
    - Milestone 3 process will complete Thursday Sept 21
    - Will go to NPRM within the next month or two
    - Was part of a 12 rule package
    - Rule and AC will come out at the same time
        - 20 series AC since it is 25/33/35
    - Timing is shooting for end of 2024 or beginning of 2025
    - Part 25/33/35
    - Part 27/29 have their own AC and compliance documents following SAE
    - Part 23 is a mixed bag similar to 27/29
        - Appears to be the ASTM standard for approach
        - Mike Vukas for Part 23 // Jon Vanhaught for 27/29 - contacts
    - Question from Stefan about CIA related to rules and SC and legacy aircraft
        - Rules will apply going forward if there is any cyber concern going forward
- Cyrille
    - Nothing new related to Part-IS other than what has been published
    - New regulation for ATM for information security
        - Regulation was published in July // need to check applicability timeline
        - Look to ED-205 to address this?
        - Will send an email about the new regulation
- Stefan
    - Rule making task 161 from EASA related to aerodrome
    - Will be similar to product security protection

Siobvan Moved on to the DO-356A/ED-203A FAQ Companion Doc and Expectations

- Revision would take a lot of time
- So FAQ was proposed to get there quicker
- EASA presented their approach
- Boeing gave a presentation as well

- Cyber Ben was tasked with putting this together
    - Has only received feedback from the AIA
- Stefan provided presentation from AIA
    - Defense in Depth for Hazardous Threat Conditions
        - Two proposals
            - Clarify that companies need to provide justification for not using defense in depth
            - OR consider providing SAL-gebra on SAL assignments
        - Major may be applicable for this issue as well
    - Limitation of Physical and operational control acceptance
        - Update FAQ to state that physical and operational controls are acceptable if evidence is provided for effectiveness and acceptable human factors
        - Maybe we delimit the security environment instead of trying to assign SAL's to physical and operational security measures
        - Varun, if physically secure, then it is a controlled environment, you should be able to quantify the physical security measure, you should be able to take credit for a physical security.
        - Stefan, need some language to allow for that credit.
        - Partick, physical should be appropriate in order to take credit for them.
        - Stefan, they do not necessarily be equate to a SAL.
        - Varun, physical controls can achieve a reduction in exposure but maint people can get in and crew can get in, need evidence that people are controlled using procedures and training,
    - Supply Chain Considerations within security assessment
        - Aircraft cannot protect against supply chain attacks
        - Proposal to adopt best practices from AIA software distribution paper and monitor RTCA/EUROCAE DSEC
- Raphael Blaize Presentation on Mapping Guidance for Common Criteria
- BREAK
- Stefan presented a Writing Style Approach guide
    - Varun, Requirements are measurable when verifiable.
    - Cyrille mentioned, EUROCAE has format as well
    - Siobvan suggested to use other persons within our orgs to get editorial help.
    - Olivia suggested to use DSEC to follow this.
    - Stefan is looking for a checklist to use for a review of a requirements document
    - Closing Plenary session.
- **DSEC Part 1 with Olivia and Hannes took on the afternoon session**
    - Cyrille Rosay mentioned that he was asked to add the link to the EASA regulation on the conformity assessment of certain ATM/ANS equipment as well as regarding the approval of organizations involved in its design and/or production: https://www.easa.europa.eu/en/document-library/regulations/commission-implementing-regulation-eu-20231772
    - Stefan Schwindt provided 3 AIA Software distribution papers:
        - 2020: https://www.aia-aerospace.org/publications/aia-civil-aviation-cyber-security-subcommittee-software-distribution-security-white-paper-2020/
        - 2021: https://www.aia-aerospace.org/publications/aia-civil-aviation-cyber-security-subcommittee-software-distribution-security-white-

        paper-2021/
        - 2022: https://www.aia-aerospace.org/publications/aia-civil-aviation-cyber-security-subcommittee-software-distribution-security-white-paper-2022/
    - Mitch Trope mentioned "*Note: Final Review and Comment (FRAC) Completion Due Date refers to the date that the committee plenary approves the document after completing the FRAC Process. SCs should submit the final document at least 45 days before the PMC meeting where it will be considered for approval"
    - Isidore Venetos added Here is where storage and functionality are integrated.... just a thought. I will stop here but I feel that data is stored to be used and accessibility and functionality needs to be considered in the lifecycle. https://datamanagement.hms.harvard.edu/plan-design/biomedical-data-lifecycle

- End of day one

Day 2 – 19 September, 2023

- SG4 ISMS Information Security Management System

- Matthew Willm provided the initial presentation for ISMS
    - Began with Asset Inventory and Classification
    - Indirect Nature of Safety Consequences
    - Proposing an iterative process
    - Went over the several assumptions about the proposed whitepaper
    - Varun, question, please clarify out of scope…
    - Matthew: it is for safety severity of asset. If it has no safety effect.
    - Varun: Traditionally, from interference perspective, it may have an effect
    - Stefan, we should have a rule to ensure consistency.
    - Matthew: This approach can be extended to other applications such as MRO
    - Next is to look at the short term safety effects
- Questions after the paper presentation
    - Anup: How do u deal w shared assets?
    - Matthew: One asset can be in different groups
    - Anup: I worry that most of our assets would be in Group one. Some clarity in the paper would be valuable
    - Stefan: this is an architectural type of question, we are not going to secure each asset individually.
    - Additional comments from Varuun:
        - In the US we don't have part-IS
        - Bilateral agreements need to be set in place
        - It has to be sorted out. It is not an AMC for the US even when it is for Europe
        - If a US company apply for dual TC FAA/EASA, can EASA enforce PART-IS as prerequisite for TC?
- Jeff Burkey FAA mentioned that soliciting feedback from stakeholders FEELS like it should be the best way to develop a path forward. However, if you ask a question on an online forum... you'll get zero response. But, the MOMENT you instead make an incorrect statement, you'll have more feedback than you'd get in months of asking.
- Siobvan Nyikos Boeing mentioned that the TOR says: Generate a new document for publication to address a management system for Information Security which supplements the current Safety Management System.
    - FRAC completion listed as June 2024, doesn't exactly leave us time to "boil the ocean" as Dave Pierce says

SG6 DO-326B and CIA

- Sarah Stern provided the initial presentation for CIA integrated into the DO-326B conversation
    - Pat and Stefan to go over changes that are needed to align 326A closer to 356A documents.
    - Varun added that the FAA rule will apply to Parts 25, 33 and 35.
    - Patrick-goal is to state that physical security measures can be used for controlling a threat.
    - Pat, addressing something like a usb port tampering, there is a standard, need to substantiate that the control is sufficient.
    - Locks/keyed locks are required for panels in aircraft, physical security

is required to protect ethernet nodes.

- Cyrille, in Europe they have a separate physical security requirement. Crew should be trained. Info sec scope is different from physical security.
- Patrick added that the operator should define what is accessible and what is not for the OEM.
- Pat added that Decomposing the word “aircraft” to ac systems or subsystems may help clarify.
- Stefan doesn’t see the value in the change.
- Varun, the STC would

- Pat added that Decomposing the word “aircraft” to ac systems or subsystems may help clarify.
- Stefan doesn’t see the value in the change.
- Varun, the STC would

- Stefan: This is related to finding the affected area before doing a CIA.
- Siobvan -- From TOR: Generate an update to the existing DO-326A to include guidance on Change Impact Analysis as it relates specifically to Information Security.
- Mike Tumminelli understand the question was more about the metamodel behind MSTM. Anyway would be very nice if we could define an extension to AADL, connecting with system and safety.
- David Pierce - Certainly there are many tools and methods, how will you decide on one or more and not others

Day 3 – 20 September, 2023

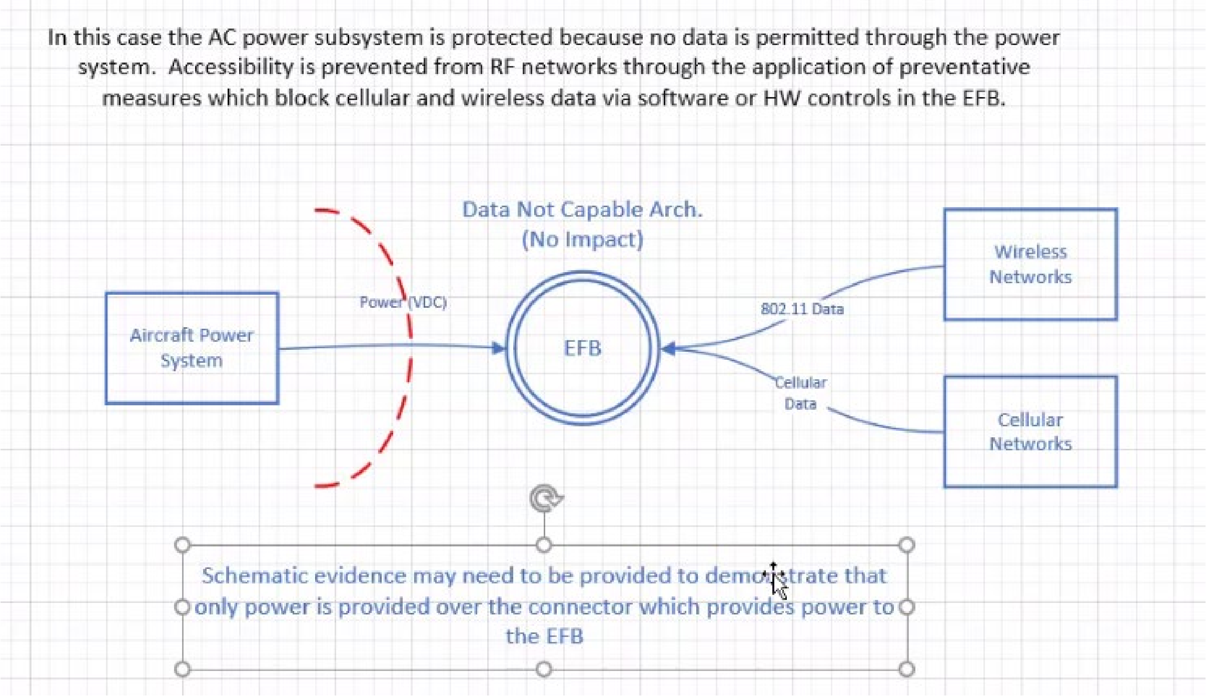
- SG4 ISMS Information Security Management System - Part 2

- Stefan picked back up from his presentation the previous day
    - Began looking toward SMS integrations
    - Several documents related to this integration
        - From Cyrille here I add some European context: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms
        - From Patrick: https://www.aia-aerospace.org/wp-content/uploads/SMS-Standard_final-issue-A_20180917.pdf
        - Also from Patrick: https://aiac.ca/wp-content/uploads/2022/04/SMS-Standard-SM-0001.pdf
        - From Cyrille again: GM1 IS.I.OR.260(a) Continuous improvement // https://www.easa.europa.eu/en/downloads/138217/en
    - Also related to the Part-IS crossover
        - From Martini: The amendments to the Authority requirements that empower the competent authority to perform oversight against Part-IS provisions are in the implementing act, so audits can start from the applicability date of the IR
- Lots of discussions about not all orgs are subject to Part-IS and most orgs differ in size

- SG6 DO-326A/ED-202B – Part 2

- Sarah Stern led the discussion along with Patrick to present several examples of how to break down attack vectors and showcase them

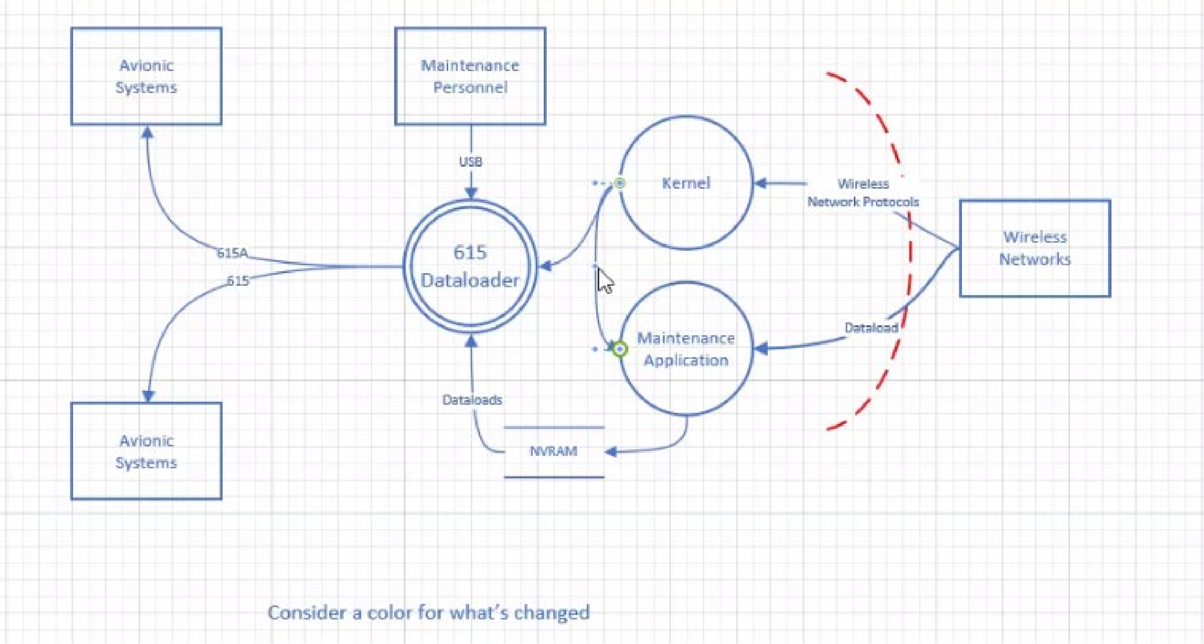
- Example 1



In this case the AC power subsystem is protected because no data is permitted through the power system. Accessibility is prevented from RF networks through the application of preventative measures which block cellular and wireless data via software or HW controls in the EFB.

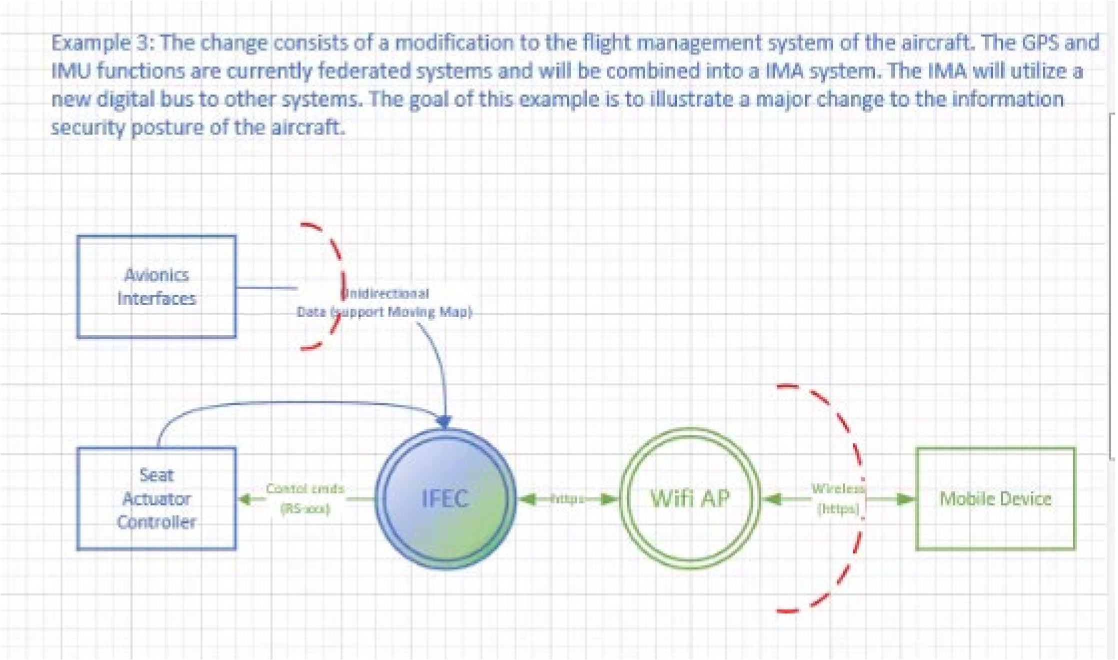
Schematic evidence may need to be provided to demonstrate that only power is provided over the connector which provides power to the EFB

- Example 2



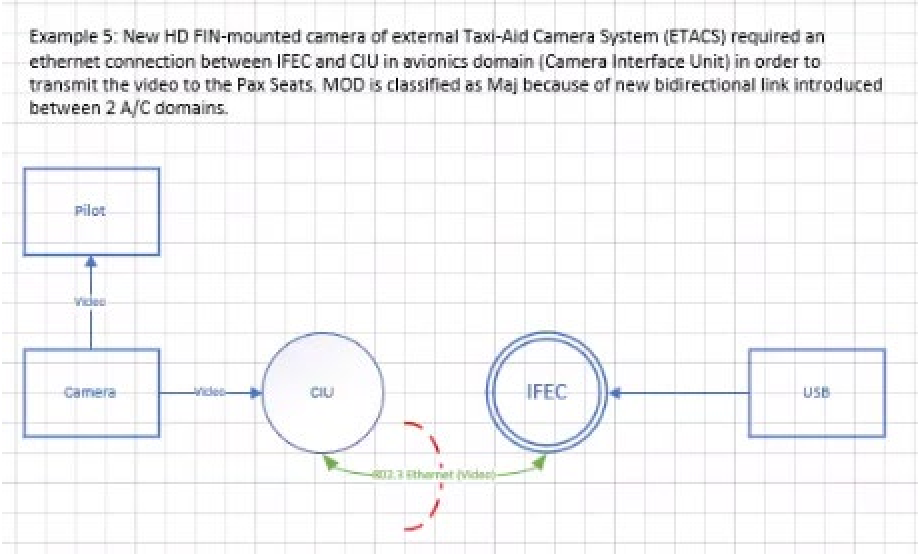
Consider a color for what's changed

- Example 3



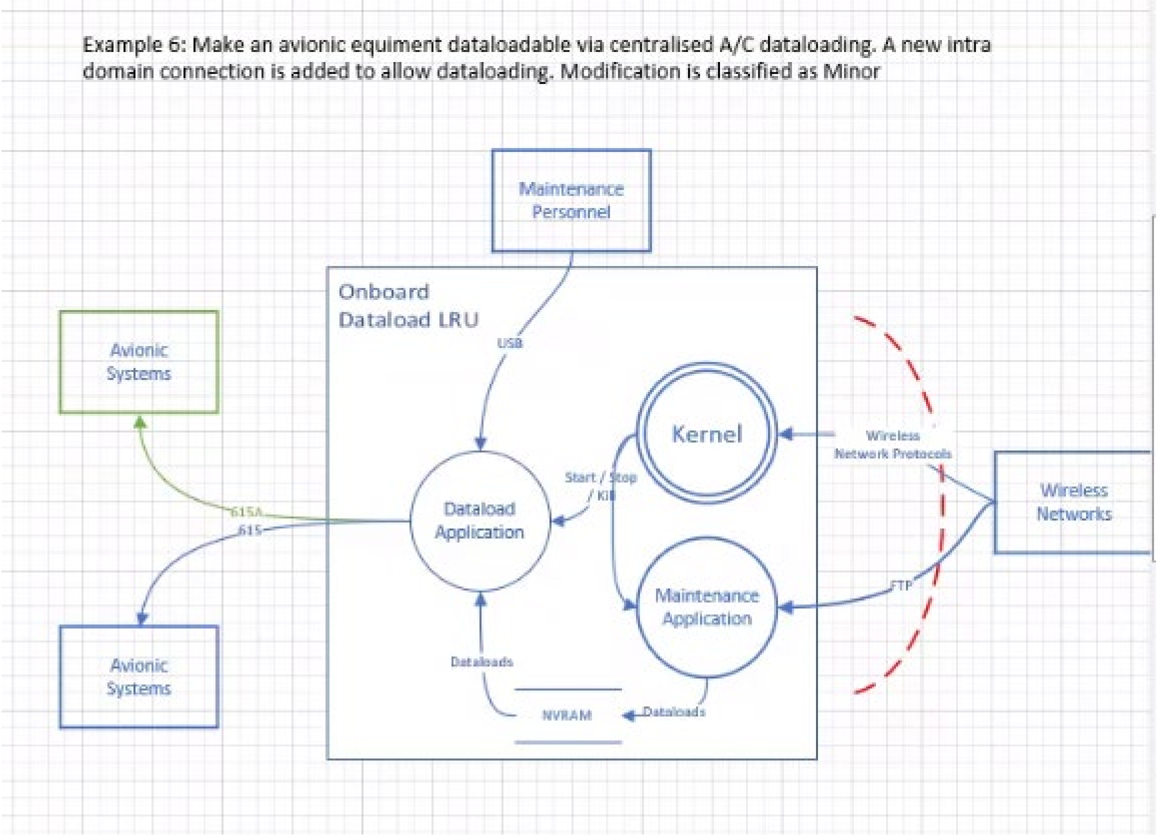
Example 3: The change consists of a modification to the flight management system of the aircraft. The GPS and IMU functions are currently federated systems and will be combined into a IMA system. The IMA will utilize a new digital bus to other systems. The goal of this example is to illustrate a major change to the information security posture of the aircraft.

- Example 5



Example 5: New HD FIN-mounted camera of external Taxi-Aid Camera System (ETACS) required an ethernet connection between IFEC and CIU in avionics domain (Camera Interface Unit) in order to transmit the video to the Pax Seats. MOD is classified as Maj because of new bidirectional link introduced between 2 A/C domains.

- Example 6



Example 6: Make an avionic equiment dataloadable via centralised A/C dataloading. A new intra domain connection is added to allow dataloading. Modification is classified as Minor

Day 4 – 21 September, 2023

- SG5 DO-DSEC - Data Security- Continued

Olivia began the discussion by going over the DSEC timeline

- Targeting first draft complete on May 2024
- Public Comment July 2024
- Release December 2024

Started going over use case that was discussed on Monday

- Aircraft Logs
- Aircraft Databases

Looking at Scope, Minimum Security Objectives, Objectives

Focused on Data Characterization, Data States and Activities

Data profiling was examined as well

Began working through the creation of the use case template to make it easier to create additional use cases

- Started with the Aircraft Database Use Case first
- Ted Patmore mentioned that risk exposure must be considered for each distribution hop type, storage, & archive...
    - Nav databases, terrain, aeronautical data bases (procedures, airspace detail, …for flight ops), weather databases, performance data bases(fuel efficiency..for flight planning), aircraft system databases(maint, config, sw updates)
- Matthieu mentioned critical database: electronic check list

- SG3 DO-392A

Began ISEM after lunch

Stefan went over CVSS V4

- https://www.first.org/cvss/calculator/4.0#

Kathleen Finke began going over CVSS from Astronics

- Use cvss for recommendation for patching (recommend a patch).
- Stefan: How do u communicate up and down the supply chain? Kathleen: we don't require CVSS analysis done by supplier. For our customers, we are responsible for our system, we provide system impact to our customer. We have placed alerts to customers on CVSS scores if we find a need to incorporate into the larger system.
- Do u provide a notice before patch, how long it takes for a patch. Kathleen, it is per contract. The patches depend on where we are in the development life cycle.

Boeing CVSS presentation-Marshall

- Manon Gaudet maybe not exposure to attack but to compromise?
- Siobvan said that yes it is more akin to compromise
    - risk is larger for a larger fleet of aircrafts-may need to add to calculation.
    - Stefan was asked what are the important things that we must look at? We should agree on these things. Such as what is acceptable.
    - Stefan was also asked what we need to find for just enough details to choose a factor. Need to find the main risk items. Need to get a balanced approach. Don't calculate something that is impossible to calculate.

Day 5 – 22 September, 2023

- WG 72 and SC-216 Plenary Day 2, 09-22-2023:

Siobvan greeted participants. This is plenary part
Sam Masri brought up the minutes from the last Plenary

- Siobvan moved to approve the minutes
- Ted K seconded

Siobvan began going over meetings coming up in the next year and remainder of 2023

- 4Q2023 will be at Honeywell Deer Valley Phoenix, AZ, Dec 4-8
    - Formal meeting notice forth coming
    - Sam Masri has a map of the area that is also going to be shared on the EUROCAE and RTCA websites
- March 2024: DO-326B/ED-202B FRAC Comment Resolution
- 1Q2024: EASA HQ Cologne, Germany, April 22-26
    - Can only accommodate 26 people
- 2Q2024: RTCA WDC June
    - EASA FAA Safety Conference second week in June
    - Need to look to A-ISAC schedule as well
    - June 2024: DO/ED-ISMS FRAC Comment Resolution
- 3Q2024: EUROCONTROL Brussels October 7th-11th
    - Shoot for the second week of October
    - September 2024: DO-392A/ED-206A FRAC Comment Resolution
- 4Q2024: ERAU Daytona Beach, FL, December
    - December 2024: DO/ED-DSEC FRAC Comment Resolution

SG3 Status

- Alain and Andrew
- Several presentations on changes to make ISEM and ISMS work together
- There is need for some additional content around risk assessment and evaluation of current risks and its tie in to event management
- This content needs to be added to the ISEM
- Try not to move things around too much as other documents already reference ISEM
- Also went over CVSS V.4 coming out soon and need eyes on
- Also there will need to be an update to the task sheet for ISEM

SG4 Status

- Matthieu presented white paper related to Ident and Classification Guidance for Part-IS Assets
- FAA/Varuun concern over signing up for more than required
- Get slides form Siobvan

SG5 Status

- Olivia presented
- Updated document timeline
- Review Scope
- Section assignments

SG6 Status

- Stefan presented
- Pat presented updates to data flow diagrams
- Explored the questionnaire
- CIA questionnaire examples 4,5,6 reviewed and presented by Airbus
- Proposal to incorporate CIA questionaire and related DFDs in Appendix
- Need to continue work on questionaire
- Discuss text alignment on DO326/DO356

    - Examples would be SAL and refutation testing

Break

RTCA and EUROCAE Cyber-Related Standards
- SC-216/WG-72 Walk through
- SC-236 WAIC

SAE Cyber

SBOM by Kanwal Reen
- Software Bill of Materials
- Being driven by executive order by the US
    - Not realistic for aviation

○