RTCA Paper No. 145-24/SC216-152
EUR. 209-24 / WG72-178

St. Denis and Washington DC, 06/24/2024

EUROCAE WG-72 Meeting #74 / RTCA SC-216 Meeting #65 Joint Plenary

“Aeronautical Systems Security” Calling Notice

Date	***Monday – Friday 22-26 April 2024*** *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	Organization	April 22	April 23	April 24	April 25	April 26
Adam Patrick	Rolls Royce	P	P	P	P	P
Alain Combes	Airbus	X	X	X	X	X
Alessandro Oteri	Leonardo Helicopters	P	P	P	P	P
Ana Pasuca	IATA		X	X		
Andrew Drake	NetJets	P	P	P	P	P
Aneesh Sankruth	Gulfstream	X		X	X	
Angeliki Karakoliou	EASA					X
Anna Guegan	EUROCAE	X				
Anup Raje	Honeywell	P	P	P	P	P
Ben Nagel	CyberBen	P	P	P	P	P
Bernard Margelin	Airbus				X	
Bill (William) Trussell	IFR Development	X				
Billy Ogunsola	CAA UK	X	X	X	X	X
Borja Garcia-Blanco Castro	EASA	X	X	X	X	X
Charles Sheehe	NASA	X	X	X	X	
Chris Gorton	CAA UK					X
Christophe Travers	Dassault Aviation	X				
Claudio Castro	Lilium	X	X		X	
Cristian Bertoldi	Airbus		X			
Cyrille Rosay	EASA	P	P	P	P	P
Darius Ashtari	Dassault Aviation			X		
David Harvie	ERAU	X	X	X		
David Pierce	GE Aerospace	P	P	P	P	P
Davide Martini	EASA	P	P	P	P	P
Daniel Salter	CAA UK				X	
Emerson Luiz Cunha	EMBRAER	X	X		X	X
Francesco Acerbi	Leonardo Helicopters	X	X			
Felix Meier-Hedde	Airbus	X		X	X	
Florin Grafu	R.A. Romatsa			X		X

Contact	Organization	April 22	April 23	April 24	April 25	April 26
Frédéric Heurtaux	Safran Group					X
Gilles Thales Descargues	Thales Group			X		X
Hagop Kazarian	Bombardier	X	X			
Hannes Alparslan	EDA	X	X			X
Ian Coaker	BAE Systems					X
Jakub Cunat	Egis Group	X	X	X	X	X
Jean-Paul Moreaux	EASA	P	P	P	P	P
Jeff Burkey	FAA	X	X	X	X	X
Jenni Rueben	Saab Group	X				
John Flores	FAA	X	X	X	X	
Jose Romero-Mariona	Raytheon Technologies		X		X	
Judicael Gros-Desirs	Airbus	X	X	X	X	X
Kanwal Reen	Collins Aerospace	P	P	P	P	P
Karan Hofmann	RTCA	P	P	P	P	P
Ken Kitamura	JCAB	X	X	X	X	X
Kevin Meier	Textron Aviation	P	P	P	P	P
Kristof Lamont	EuroControl					X
Laurent Leonardon	Collins Aerospace	X	X	X	X	X
Lee Howard	Honeywell	X	X	X	X	
Ludovic Donnadieu	Airbus					X
Manon Gaudet	IATA		X			
Marc Lord	Department of National Defence of Canada	P	P	P	P	P
Marcos Ramos	Embraer	X				
Mario Lenitz	Austro Control	X	X	X	X	X
Mark Kelley	Belcan	P	P	P	P	P
Marshall Gladding	Boeing	X	X	X		
Martin Call	Boeing	P	P	P	P	P
Matthieu Willm	Dassault Aviation	P	P	P	P	P
Mike Tumminelli	Gulfstream	X	X	X	X	
Mila Obradovic	ECN				X	
Minh Trang	Airbus				X	
Mitch Trope	Garmin	X	X	X	X	X
Neset Sozen	CMC Electronics				X	
Nicolas Durandeau	EASA	X		X	X	X
Nikita Johnson	Rolls Royce	P	P	P	P	P
Nivethanan Sivanathan	CAA UK					X
Olivia Stella	SWA	P	P	P	P	P
Pascal Manguer	Dassault Aviation			X		
Patrick Morrissey	Collins Aerospace	P	P	P	P	P
Peter Tsagaris	TCCA	P	P	P	P	P
Phil Watson	Panasonic	P	P	P	P	P
Philippe Dejean	Safran Group	X	X			X
Prachi Shekhar	EGIS Group				X	
Richard Nguyen	Boeing	P	P	P	P	P
Romuald Salgues	Airbus Helicopter	P	P	P	P	P
Rosemberg Andre da Silva	ANAC-Brazil	X	X	X	X	X
Sam Masri	Honeywell	P	P	P	P	P
Sarah Stern	Boeing	P	P	P	P	P
Siobvan Nyikos	Boeing	P	P	P	P	P
Stefan Schwindt	GE Aerospace	P	P	P	P	P
Steve Hofmann	CCxH	X	X	X	X	

Contact	Organization	April 22	April 23	April 24	April 25	April 26
Tara Knight	SWA			X		
Ted Kalthoff	Archer Aviation	X	X	X	X	X
Ted Patmore	Delta	X	X	X	X	X
Thomas Parmer	FAA			X	X	
Thuan T Nguyen	FAA	X	X	X	X	X
Varun Khanna	FAA	X	X	X	X	X
Yildiz Uludag	TÜBİTAK	X				

Day 1 – 22 April, 2024

Welcome/Introduction - Gian Andrea

SC 216 announcement - Siobvan/Cyrille/Patrick

EUROCAE/RTCA slides - Anna/Karan

Add validation of the previous minutes - Sam

Tour the table, expectations for the week - All

Updated SC-216 TOR (Rev 17) / WG-72 task sheet approval - Siobvan/Cyrille/Patrick
- Anna says we need to align on the title of the reports before we update the TOR
- Karan also warned that we need to be as realistic as possible on the time table for the documents, Changing dates a lot causes issues with PMC
- Anup - how are the documents the same but there have been some changes
- Nicolas - There was a non-concur with some objectives related to validation
- Three items - selection of the COTS / hardening of the COTS / Testing of the COTS

Regulatory update EASA - Nicolas

Position on CS-23/ASTM/standards - Nicolas
- Anup - how are the documents the same but there have been some changes
- Nicolas - There was a non-concur with some objectives related to validation
- Three items - selection of the COTS / hardening of the COTS / Testing of the COTS
- Cyrille recommended that Marie Chantel give an overview of ED-305 and what the WG-112 is putting together

Regulatory update FAA - Varuun
- Legal approve and MS3 has been pushed to the executive level at the FAA and will soon be out for public comment
- July is when new rule will be released

Position on Part-23/ASTM/standards - Varuun/Mike Vukas
- From Mike -
- Using ASTM will with Part 23 makes it so no special condition is required
- There is a Part 23 Policy Statement that pushes the need to go to Admt 64
- Class 4 can use ASTM but can step up to RTCA if they wish
- Anup asked about bi-lateral between EASA and FAA related to ASTM
-- Varuun and Jeff Burkey will run down the answer for this and get back to us

SG 4: ISMS

Stefan and Romuald Salgues- Romuald presented the Airbus Helicopter pilot project lessons learned. Discussions amongst participants underlined the importance of including diverse organizations, both small and large, beyond just those involved in Smartboards or design-focused areas. They highlighted the necessity of ensuring that ISMS covers all organization types to reflect the varied needs within the industry. The discussion also pointed out the ongoing efforts in various countries to develop nationalization programs, advocating for a broader approach rather than focusing solely on specific methodologies like freeway-focused ones.

Key insights from more mature organizations that are already implementing Safety Management Systems (SMS) were discussed to form future strategies. The goal is to integrate this feedback while addressing the unique needs of smaller, less complex organizations. Additionally, there was a strong call for drawing parallels with existing frameworks and identifying potential synergies to ensure that current systems are appropriate and effective.

Consistency in implementation and auditing across different countries and authorities was identified as a critical need. Participants suggested the adoption of standardized procedures and policies to achieve uniformity, potentially drawing from international standards such as ISO. This approach aims to streamline the process and ensure a coherent application of rules and practices.

The pilot project's progress since June 2022 was reviewed, noting the iterative process of analysis and feedback. Monthly meetings have facilitated comprehensive discussions and adjustments, leading to the development of compliance proposals. The outcome highlighted the importance of starting with organizational structure and management interviews in new projects, and ensuring a consistent approach to audits, possibly by adopting internal procedures or standardized guidelines.

Varun- What was the primary objective of this exercise? Was it to evaluate the effectiveness of our current practices, or to identify areas that need improvement? What was the fundamental goal of the pilot case?

Romuald Salgues- The pilot project focused on two primary objectives from the EASA side. Firstly, from the authority perspective, the aim was to evaluate the completeness. This included checking if any issues were overlooked during the drafting process despite multiple rounds of commenting and editing. Secondly, for the organizational perspective, the objective was to ensure a thorough understanding of how the guidelines fit into the existing implementing rules for auditing organizations. This involved verifying that the processes developed were appropriate for compliance and interpreting the new requirements correctly.

Romuald Salgues- The lessons learned highlighted that integrating an SMS (Safety Management System) can be done either partially or fully, depending on the organization's needs. Full integration isn't always effective at 100%, so it's crucial to use different tools and approaches to tailor the SMS integration process. The decision on whether to implement SMS at an organizational level or in other ways is up to each organization. It's important to engage in discussions with business stakeholders to determine the best approach and that works for them.

Stefan discussed the importance of effective communication and collaboration between different aspects of integration within the organization. While certain aspects may share common goals and can be integrated seamlessly, such as identifying people's risks and roles for training purposes, others may require a more nuanced approach due to differing perspectives and requirements. For example, the process of risk assessment varies significantly between cyber and safety perspectives, necessitating distinct methodologies and mindsets. However, effective communication remains essential for understanding the impact of one aspect on another and for ensuring a holistic approach to integration.

Romuald Salgues added that the point being conveyed in the conversation is that while certain aspects may appear similar or align conceptually, they are fundamentally distinct processes with unique characteristics and requirements. He emphasizes that these processes do not necessarily complement each other or serve the same purpose, despite initial appearances suggesting otherwise. They assert that each process stands alone and has its own significance, highlighting the inherent complexity and beauty in their individuality and functionality.

The discussion highlighted the importance of ensuring alignment and communication between different systems within the organization, such as ISMS, SMS and other structures. Overall, the goal is to identify common principles across systems, such as risk management, to ensure cohesion and efficiency in organizational processes.

It's crucial to ensure that the processes we design meet organizational needs and standards, particularly when it comes to certifying our products for public use. Trust is paramount here. No matter how secure our devices are, if the organization delivering them isn't trusted, it undermines the entire process.

So, the question becomes: How do we maintain trust throughout the supply chain? It seems like auditing suppliers' processes and products is a key step. This allows us to trust their deliverables without needing to delve into sensitive details. Is that the idea?

There was a discussion that revolved around the exchange of specifications with suppliers in digital formats and the importance of ensuring compliance with contractual requirements.

Stefan highlighted the need for suppliers to independently determine their compliance.

The group discussed examples, such as the validation of software installations to prevent the transmission of malware. Additionally, there was a focus on the importance of verifying the authenticity of digitally signed materials. Overall, the conversation underscored the significance of robust verification processes to ensure the integrity and security of supplied products and services.

Mario Lenitz- Some of the key points discussed:

- SMS and ISMS must communicate effectively, whether through partial or full integration. Approved organization audits are necessary to monitor compliance with Part-IS requirements, providing feedback to ensure corrective actions are effectively implemented.

- Organizations must identify and categorize relevant contracted organizations involved in implementing the ISMS. Oversight and reporting should cover aspects such as the number, size, activities, and maturity level of contracted entities.

- To ensure all relevant processes of the Design Organization are addressed, a structured assessment progression scheme is discussed. This scheme visualizes the assessment process for development, testing, certification, configuration management, and other relevant areas.

- Organizations must ensure assessments are regularly updated and detect critical changes before the next recurrent assessment. Insider threats should be considered in risk assessments, with different levels of personnel trustworthiness required based on activity criticality.

- EASA requested that organizations describe their risk assessment processes and management of risk treatment plans. This includes setting up processes for regular checks on security measures' effectiveness and conducting stress tests to ensure robustness.

- IS.OR.220 outlines requirements for detecting, responding to, and recovering from information security incidents. EASA may check that organizations record all non-exploitable vulnerabilities with catastrophic effects and regularly reassess them.

- Internal organization audits must consider security aspects alongside Part 21 competencies. Response to findings is defined in Part 21.B.433, and security considerations may be added by EASA.

- EASA confirmed the availability of a rule for secure communication of sensitive information by September 2025. Organizations contracting ISMS activities must maintain a separate communication channel for critical suppliers.
- Independence between the compliance manager and ISMS officer is required. Organizations must assess the competencies of personnel involved in Part-IS functions and provide tailored awareness and training.
- Record keeping for staff qualifications and experience is essential, with defined re-assessment criteria for recorded security events. Change approval processes must be agreed upon by EASA, including classification criteria and examples.
- Essential elements must reach a maturity level of "Operating" when the rule becomes applicable. EASA is discussing internally the list of these essential elements, expected to be available by summer 2024.

Varun- Should integrate cybersecurity measures into existing processes. The speaker emphasizes leveraging current practices and relationships between suppliers, buyers, and operators to ensure robustness against threats. They advocate for augmenting existing systems with cybersecurity protocols rather than implementing excessive regulation, highlighting the need for verification and the challenges of monitoring multiple interfaces. The focus is on encouraging companies like "Collins, Honeywell" to incorporate cybersecurity seamlessly into their established systems for quality control and supplier management.

Mario Lenitz- EASA is collaborating with other EU member states' competent authorities for an AMC/GM update, with collection of inputs expected to be completed by the end of 2024. Mario also presented the list of selected organizations for the EASA pilot cases.

Stefan- Presented the DO-/ED-ISMS:

Stefan highlighted that implementing an Information Security Management System (ISMS) encompasses several key components. Firstly, a comprehensive risk assessment is conducted to identify potential threats to the organization. Followed by establishing risk controls to mitigate these threats effectively. Monitoring mechanisms are then implemented to ensure that security measures are continually effective and optimized. Policies are developed to communicate roles, responsibilities, and expectations to all stakeholders, ensuring clarity and alignment. Incident detection, response, recovery, and notification procedures are crucial aspects covered in subsequent training modules. It's essential to recognize that risk assessment, controls, and monitoring are interconnected with incident response, recovery, and notification, highlighting the holistic nature of ISMS implementation.

There was a concern about the challenge posed by multinational corporations. Often, only a portion of the company is directly affected by certain regulations, while the rest might face unnecessary hurdles. This discrepancy can impede progress and frustrate both internal processes and customer relations.

How can we establish sustainable solutions that strike a balance? Take, for instance, a company like Collins, which already adheres to rigorous government requirements. Crafting a basic minimum standard that fulfils regulatory obligations without imposing excessive burdens is crucial. We need an approach that efficiently addresses compliance without becoming an overwhelming administrative burden.

Stefan- The primary objective of risk assessment is to systematically and comprehensively identify potential risks. Outcome No. 1 pertains specifically to aviation safety risks, while Outcome No. 2 encompasses all other types of risks. It is imperative to adequately mitigate resultant risks, which are determined by the product of severity and likelihood. Regarding severity, aviation safety risk should be evaluated using standardized values such as CAT-HAZ-MAJ-MIN, while the challenge lies in maintaining the realism of scenarios, including determining acceptable cutoffs. Non-aviation safety risks can be categorized based on organizational preferences or relevant regulations. Quantifying likelihood poses challenges similar to severity assessment, with considerations for different time horizons—short versus long lifecycles. Long lifecycles involve controlling defense and risk mitigations without the ability to measure or react to threat sources directly, as exemplified in aircraft certification processes. Conversely, short lifecycles allow for flexible responses to threat sources, but measuring these sources and justifying flexible approaches remain ongoing concerns.

In previous discussions, the concept of "distance to aircraft" has been explored, offering potential solutions through suitable architectures for mitigating risks, which involve a trade-off between the number and performance of controls. Additionally, some organizational structures have found methods for correlating threat to severity. ISO27005 presents a risk management process that should be widely adopted, though it doesn't directly address severity, likelihood, or risk acceptance, but rather suggests defining these aspects in specific clauses. Moreover, it doesn't guarantee consistency or comparability with other systems but advises considering these factors. Conversely, NIST provides risk models and tiers, serving as an informative foundation. It quantifies values such as vulnerability and threat occurrence, yet the inherent subjectivity of quantitation prompts questions about achieving objectivity for external consensus, particularly concerning low and high levels of threat intelligence and bridging information gaps.

Billy Ogunsola- Questions whether the concerns being discussed are addressed by Article 5 of the relevant document. If anyone has reviewed Article 5 and if it's possible that some of the concerns have already been addressed within it. He also mentions that Article 5 may pertain to concerns originating from outside the European Union.

Stefan- The discussion revolves around the issue of authority and influence within organizations, particularly in the context of regulatory mandates. Stefan mentioned that not everyone is mandated, regardless of whether they are part of an approved organization. Stefan acknowledged that the varying degrees of leverage we have with different suppliers, citing examples like Microsoft, Amazon, and Google, who might not be responsive to our demands due to their market dominance. Stefan also discussed the challenge of dealing with incomplete information from suppliers, particularly when technical capabilities are lacking.

Billy- The observation made here was regarding the importance of asset classification in the risk assessment process for organizations. Billy suggested that before identifying threats, it's essential to classify assets because understanding the value and importance of assets is crucial for assessing the potential impact of threats. Billy proposed adding asset classification as a preliminary step in the risk assessment process, emphasizing its role in facilitating a more comprehensive understanding of organizational risks.

Siobvan- Asks Billy, whether there are any existing resources they can review to identify assets for consideration.

Billy- Yes, I can make contribution to that if you want me to.

Stefan- Additional considerations in risk assessment include ensuring completeness and accuracy throughout the process, particularly in addressing all assets which may change frequently, especially in IT/OT environments where configuration management expectations may be lower than in aerospace. An iterative approach is essential as assets in scope will evolve with architectural and security measure implementations. Stakeholders may require education to identify safety impacts effectively. Assessment directionality must encompass both functional safety impacts influencing IT/OT and vice versa, necessitating clear documentation for compliance, including evidence of scope, asset identification, and risk approach, often supplemented by diagrams. Establishing processes or triggers for updates is crucial, whether change-driven or periodic, considering the dynamic nature of partnerships, customers, authorities, and assumptions concerning physical security. Ultimately, consistency demands a unified risk assessment approach to ensure coherence and comparability.

End of Day One

Day 2 – 23 April, 2024

SG 5: DSEC

Data Security - Hannes/Olivia

- Hannes began with going over questions related to the direction of the DSEC document and what we want as a committee for it to look like
- Varuun wants to ensure we have a consensus position
- Cyrille says it is hard to have engagement with people that don't feel the topic is relevant to them
    - European groups feel that there is no benefit to them with the document
    - The current use case we are developing appears to be leaving large parts of the committee out
    - There is a working group on the European side developing some work related to this, so is this document still needed?
- Varuun said the fundamental reason for this document is that there was already two hacks that have been attempted
    - The process with use cases is not popular
    - Would rather use a criteria based approach and focus on location of data
- Stephan wants us to make sure we are looking toward future issues and not getting hung up on issues that have already occurred
    - Varuun wants us to make sure we deal with issues that are occurring now as they are still happening
- Hannes is worried that maybe the issue we are trying to solve doesn't belong in this document
    - Patrick wants to understand how we are not aligned
    - Hannes looked to future connectivity
        - Currently we are just looking at dataloading
        - Patrick is concerned that people are getting hung up on this use case and not looking to expand it
- Siobvan brought up the TOR requirements
    - Mentioned that maybe the information needs to transferred into other documents
- Anup brought up the point that we are not focusing on data loading, but protections along the entire supply chain life cycle of the aircraft data
    - The data loading use case was just one part
- Stefan says we really need to focus on the threats that exist instead of just making standards to fill the space
    - We are currently missing ARINC solutions between supplier and OEM's
- Martin brought up the fact that we don't want to be to focused because then the attackers can take over everyone
    - Focus on technical solutions that are higher level general guidance
- Kanwal - DSEC document was separated so that it applied to everyone, putting the info into DO-355 means that we remove that applicability
- Varuun - if we have all of these standards dealing with this issue, then how did we have two escapements?
    - Need this standard to help handle security across the entire lifecycle chain
- Andrew - agrees with Varuun, MRO's vary widely
    - Does not want to have separate documents between US and Europe
    - Need input if we want a top down document, went with data loading use case because that was where the inputs were coming from
- Ted Patmore says we need a straw horse (outline/framework) for this document so we can move forward

    - Could be tied to ARINC SDL (software data loading) approach
- Patrick is worried about how we ensure enforcement
- Cyrille talked about how there is a sub-group that focuses on implementation and how enforcement of that implementation is done.
    - This framework is needed to assist with this enforcement
- Olivia asked for a vote to identify the approach the group wants to take
    - Vote agreed to keep the group together instead of splitting the group apart
- Siobvan provided the identified approaches:
    - Keep DSEC and path worked over past year
    - 2. Keep DSEC and rework scope -> need input from impacted stakeholders!
    - 3. Rename DSEC to better align with path worked over past year (and then create a new DSEC to address earlier priorities?)
    - 4. Don't do DSEC as there is coverage via other docs; transfer work done so far to DO-355B revision and reference Spec 42, ARINC, etc.
    - 5. Split between US and EU? Harmonized guidance is preferred
- Martin wants to borrow from infosec
    - The military has been doing this for decades
    - Protect data in motion and dat at rest
    - Then categorize the data
- Phil Watson is concerned about cases where there is no connectivity
- Andrew brought up the PCI use cases and how they have resolved data security
- Olivia mentioned that if we are going to pivot, we need to have a framework today, otherwise we will not finish by the end of the year as asked for in the TOR

Hannes began to showcase the Future Connectivity Report from the EU/US Task Force that was created by EASA/FAA/Boeing/Airbus

BREAK

Olivia started the next section with listing out the TOR actions from both RTCA and EUROCAE:
• "Generate a new document for publication addressing minimum standardsfor the generation, storage, and delivery of data, including Operational Flight Programs, sensitive maintenance data records and other security relevant data."

" The Standard on Aviation Data Security will provide specific technical details and timelines for the protection of data (executables, databases, data load activities, sensitive maintenance data, etc.) from malicious actors. "

Hannes asked for volunteers to get the framework document created:

- Cyrille
- Varuun
- Kanwal
- Ben
- Laurent
- Action to reach out to Kristof and Mario for more inclusive industry involvement.

Stefan shared some reference material for the Future Connectivity Paper:
This should be the link for reference material including the future connectivity paper:
https://eurocae.sharepoint.com/sites/strato/76ac1865-0aad-ed11-aad0-000d3adea767/6e0e1f64-0aad-ed11-aad0-000d3adea432/SitePages/Documents.aspx?RootFolder=%2Fsites%2Fstrato%2F76ac1865-

0aad-ed11-aad0-000d3adea767%2F6e0e1f64-0aad-ed11-aad0-000d3adea432%2FDrafts%2FReference%20Material&FolderCTID=0x01200023C7447583CF264EA58BD229CF52D847&View=%7BCEEC35A8-BFBE-42D3-817B-BF61FE9CC67F%7D

Hannes/Cyrille began with the Framework proposal

LUNCH

After lunch the group split up to continue the DSEC conversation and

From Olivia:
1. Identify the assets
2. Conduct a risk assessment
3. Identify the data category via the C-I-A

Siobvan noticed that 1 and 2 are part of ISMS, recommended borrowing from the DO-ISMS

Siobvan also provided excerpts from the draft DO-ISMS:
From draft DO-ISMS with excerpts from ED-201A: Information Security Risk Assessment
TBD (Information Security Risk) Conducting security risk assessments can help identify vulnerabilities, threats, and their potential impact on safety critical systems and data.
Objectives:
· [ED-201A O2-1] Document all identified functional chains to be assessed and identify all assets, interfaces, resources and stakeholders both internal to the Organization and external (supply chain, service provider, etc.).
· [ED-201A O2-2] Classify and document the criticality of all relevant resources.
· [ED-201A O2-3] Identify acceptability of risk framework that are used by external agreements.

Martin brought forth information from DO-355A and DO-356A in regards to the different definitions we have for software in our standards:

From DO-355A: The term airborne software as used in this document refers to all software that is carried aboard an Aircraft certified system. This includes binary applications as well as databases, firmware (including configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware), and configuration files. This document addresses only airborne software that can have effect on aircraft safety.

From DO-356A: Field-Loadable Software (FLS) including User Modifiable Software (UMS), Aeronautical Databases (ADB), Flight Operations Software (FOS), and any Airline Support Data (ASD) are external data that are transmitted through the aircraft dataloading functions from the external interfaces that support maintenance. These external interfaces should be assessed for security and added to the security perimeter and threat identification.

Ted Patmore added the following:
Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (often abbreviated as "CIA" or "CIAAN")

Siobvan noted that:

Generate a new document for publication addressing minimum standards for the generation, storage, and delivery of data, including Operational Flight Programs, sensitive maintenance data records and other security relevant data.

Olivia captured the key points to focus the use case on:
The 3 current use cases:

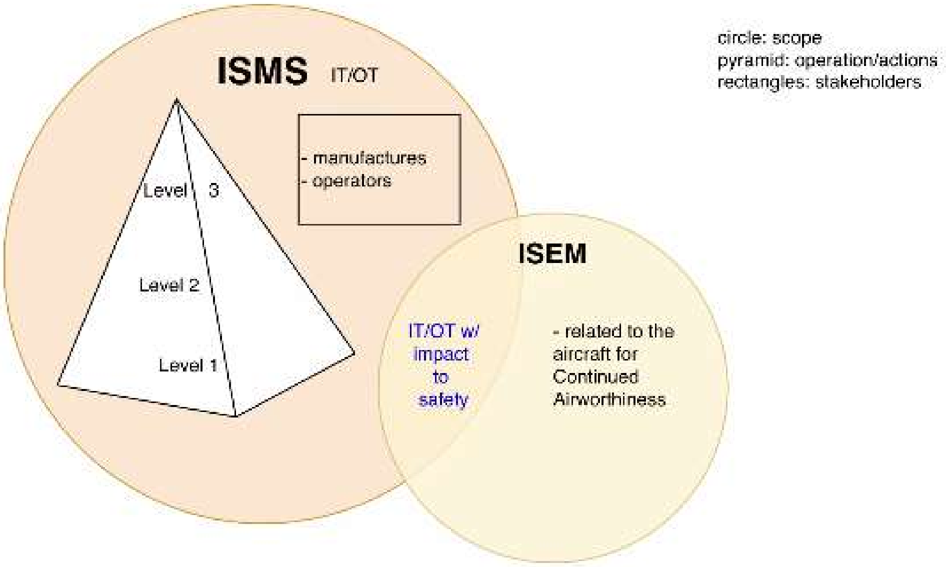
- Airborne Software Data
- Airborne Database Data
- Aircraft Logs Data
- Data Egress

Day 3 – 24 April, 2024
- SG3 DO-392/ED-206A

Andrew started the SG-3 presentation with a discussion of the objectives for ED-206A and DO-392

The objective is to standardize scoring as much as possible.
Anup suggested that we use objectives to establish a common criterion for scoring.
Stefan highlighted the need to establish a level Plainfield.

A discussion around clarifying the relationship between ISMS and ISEM. It begins with praise for graphic design and quickly moves into a discussion about whether a Venn diagram would effectively illustrate the intersection of these systems. Stefan suggested that ISEM largely overlaps with ISMS, except for a specific aspect related to airworthiness. Technical details are briefly discussed, including terminology alignment and document revisions related to performance requirements for event reporting. The conversation also touched on different organizational approaches and risk tiers according to NIST SP 800-30 guidelines.


ISMS
IT/OT
- manufactures
- operators
Level 3
Level 2
Level 1
ISEM
IT/OT w/ impact to safety
- related to the aircraft for Continued Airworthiness
circle: scope
pyramid: operation/actions
rectangles: stakeholders

Felix presented related to preparing for vulnerability management and incident management.

Martin Call, EFB failures as presumed minor will not affect the aircraft. The operator is ultimately responsible for its safety. The operator role is limited to the communication handling part that is provided by the aircraft for the EFB.

In some cases, the operator is only responsible for getting the logs but doesn't know the impact on the aircraft.

Martin Call: For a maintenance device, that is infected, it is connected to the plane, how do we manage this event?

DO-392 would answer the question. The operator reports the incident to the OEM and the OEM does the analysis or send the info to their vendor.

From EUROCAE, the update to ED-206A is needed to provide guidance to vulnerability scoring. The initial methodology present in the current version of the standard is weak in its capability to identify how information security vulnerabilities can pose a risk to aviation in particular on safety. A standardized methodology, based as mush as possible on existing vulnerabilities scoring would allow all stakeholders, including the component authorities, to ease assessment of the course of actions to mitigate the risk introduced by the vulnerability.

From RTCA, the TOR calls for the group to generate a document revision for publication to address performance requirements for event reporting.

Delivery date to PMC of this revision is September 2024.

LUNCH BREAK

- SG6 DO-326B/ED-202B

Patrick reminded the group that FRAC comments represent your company comments and should focus on the scope and context of the document.

Started by going over the comments that had been made against the current edited version.

Summary of comments:

- Non-Concur – 32
- High – 121
- Medium – 111
- Low – 112
- Editorial – 255
- N/A – 0
- Substantive – 0
- Total – 631

Sankruth, Aneesh 4/24/2024 5:25 AM •

Stefan: Can you elaborate "no need to create any material" do you mean for it to include the plan and summary updates?

Discussion around the inclusion of table 4-1. Some say that it is a very useful table. Some would like to remove it. The question came up when do you start cert.

Sankruth, Aneesh 4/24/2024 5:37 AM • The way that I understand this section to mean, someone wants to make a change to an asset either already in scope of a previous certification with security SCs or a change to Legacy aircraft on assets that have I-DAL of A/B/C

It is extremely necessary to formally establish that there are no impacts to security from these changes with data more than a plan or a preliminary CIA.

Sankruth, Aneesh 4/24/2024 5:42 AM • DO-356A should not be given the responsibility to determine what data submittals are necessary for what level of change. It's (rightly) DO-326's job.

Sankruth, Aneesh 4/24/2024 5:46 AM •

Patrick: Do you also include assets outside of the ACD in the definition of "STC"?

Action to Martin Call to propose few words.

FAA suggested creating a special classification for software is proposed to address low DAL SW that has high SAL security measures.

EASA expressed their position that from their point they are okay with current DO-356 SAL requirements. There is no need to upgrade DAL level because they include high SAL SW.

FAA added agreement. From FAA perspective, they need to figure out their process to ensure SAL controls are looked at. FAA has indicated that they would like to do that.

EASA said that DAL level ensures that the item functions as designed. SAL Levels are security related.

We will close the NC by taking the action to include a proposal for a solution into the future FAQ document.

EASA added that this is not the place to make the agreements/alignments between the authorities. They will do it by themselves.

Aneesh S: From my view, I see whatever being removed from the list of exclusions from this document going right back into a future PSecAC at the aircraft level.

It will have to be reconciled with both certifying and validating authorities on a case by case basis, which lowers the usefulness of this section.

Lee Howard 4/24/2024 8:31 AM • C159E requires SAL 2, but it also requires one to implicitly trust the service provider

Philip Watson (Panasonic) 4/24/2024 8:32 AM • Also the second sentence needs clarification: "within" what?

Lee Howard 4/24/2024 8:32 AM • for safety service over Block 1 service

Siobvan Nyikos 4/24/2024 8:35 AM • This document covers security of aircraft and does not provide solutions for organizations and services that aircraft interfaces with. It is not meant to address IEUE unrelated to assets within the aircraft boundary.

Philip Watson (Panasonic) 4/24/2024 8:38 AM • I like how that removes the list of entities. The point is the aircraft only.
But could rephrase 2nd sentence to "It is only meant to address IEUE related to assets within the aircraft boundary."

CyberBen 4/24/2024 8:39 AM • Define IEUE

Philip Watson (Panasonic) 4/24/2024 8:39 AM • Ah, should have been IUEI

Gilles Descargues 4/24/2024 8:40 AM • @@Intentional Unauthorized Electronic Interaction

Philip Watson (Panasonic) 4/24/2024 8:40 AM • Last sentence should add words "this document" so it reads "contained within this document is sound,"

Day 4 – 25 April, 2024

- SG6 DO-326B/ED-202B - Continued

Varun stated that the FAA will release a policy letter instead of an issue paper because it will be general and not project-specific. Patrick emphasized that SAL should ensure systems are functioning as intended. Boeing noted that there's less rigidity in the SAL assignment. Stefan emphasized that systems need to be evaluated individually, mentioning a specific regulation. Varun mentioned that the FAA's position on a specific project will take more time to develop. Stefan volunteered to write a policy statement white paper. Later, there were technical discussions, agenda updates, and reminders about the schedule.

Non-concur comments on DO-326A were discussed, starting with one from RR.

Philip Watson (Panasonic) 4/25/2024 12:46 AM • While I agree with the BLP principle, I disagree with the example of "DAL E no read from DAL A in flight" for reasons you mention: existing need/implementation to share data.

Rather, an appropriate solution would be "DAL A should not transmit sensitive information to DAL E".

NC Resolution: Action is to take out the models, develop concepts about data flow and control flow, and use DAH instead of OEMs. (integrity vs confidentiality). The principals will be in ch 3, EASA added to remove specific modelling names from the document. Move DFD and make it into an appendix.

Moved onto Dassault Non-concur.

June plenary should have the terms of reference addressed to include FAQ document. FAQ is being used to resolve some NCs for DO-326A update.

“Security can include physical controls” should be added to the DO-326A updated text.

FAQ document may add that text.

Proposed resolution: Resolve in the FAQ document. Here in 326A, take out the “white box” note. Remove Lines 1238 to 1304 and the positive testing part. Add info to the FAQ document.

When making a change to a type design you are subject potentially to new requirements. You have to do an evaluation to see if it is a significant change, if security involved, you would have to do security.

Plan is go over remaining comments during future biweekly meetings. Dave suggested that he would try to resolve some of the comments that are clear to address.

Sounds like we will be able to finish the document in June.

LUNCH BREAK

Afternoon:

Stefan presented a series of slides around Risk Controls and provided recommendations for securing around gaps.

Airbus presentation-Felix

The presentation given outlines the requirements and considerations regarding information security risk assessment for interfacing organizations, particularly in the context of Regulation (EU) 2023/203 or Regulation (EU) 2022/1645. It delineates two categories of interfacing organizations: those subject to these regulations and those that are not.

Key points include:

1. Identification of Interfaces: Organizations are required to identify interfaces with other parties such as service providers, supply chains, and third parties, considering data exchange and asset usage that could lead to mutual exposure to information security risks.

2. Requirements for Interfacing Organizations: Different obligations are outlined for suppliers, customers, and service providers concerning security measures, notification of vulnerabilities, incident support, and risk assessment.

3. Streamlining Risk Assessments: Due to the potentially large number of interfaces, a method of inventory and classification based on criticality is necessary to adapt the thoroughness of assessments. This involves minimizing the repetition of assessments for similar organizations.

4. Consistency of Assumptions and Objectives: There's an emphasis on ensuring consistency of assumptions and objectives between interfacing organizations to meet respective goals and ensure mutual understanding.

5. Inventory and Classification of Organizations: This involves identifying interface types, organization types, payload types, link types, and criticality levels to determine the appropriate level of assessment.

6. Example of Assessment Levels: Different levels of assessment are proposed based on criticality and interface type, with corresponding cybersecurity maturity levels and security policies.

Overall, the presentation highlights the importance of thorough risk assessment and management in ensuring information security across interfacing organizations, with a focus on adaptability and consistency.

Discussions explore the concept of supplier-customer interfaces, highlighting that organizations can switch roles depending on the context of their interactions. For example, an OEM may act as a supplier to airlines by delivering hardware or aircraft but also as a customer when airlines provide information. The discussion also mentions the classification of interfaces based on functional chains, including internal contracted resources managing safety-relevant assets remotely. It emphasizes that organizations must consider risks from both suppliers and customers.

Discussion about supplier interface risks, particularly focusing on compromised inputs and outputs that could affect organizational safety and operations. Key points include the necessity to identify safety-relevant assets from external interfaces, the importance of receiving and reacting to event notifications from suppliers, and the need to assess and mitigate risks associated with compromised inputs and outputs. There's also a discussion about the obligations of organizations to report security events to design approval holders and to provide guidance to customers regarding handling safety-related assets. Additionally, considerations are made about the challenges of obtaining information from different types of suppliers and the need for tailored solutions that accommodate the varying interests and capabilities of different organizations. Overall, the conversation emphasizes the complexity of managing supplier interface risks and the importance of developing effective strategies to address them.

Mathew/Dassault went through a proposed solution that Airbus presented in how to streamline risk assessments with organizations in interface.

Certification or can be part of an audit program so that these assumptions are justified with some rational can be verified it out here but not realistic interface does all these digital risk assessments and then from that individual set of security controls that they want to push to the other side we have to somehow standardize and then operationalize that included into the blue organization working environment here and use cases about security maturity of suppliers etcetera so that's the basic idea you're OK but you are that's OK for me so make your next line commands

Question: Mario: He thinks that the functional chain is a two-way role. OEM delivers the A/C. The airline will supply the info about events/vulnerabilities, your goal is different whether you are the supplier of the OEM.

Patient so you say security instructions and recommendations probably is more is more than having instructions from customers also everything we need to inform your suppliers about any kind of vulnerabilities.

Next steps for ISMS.
Presentation is at the Eurocae ISMS link.

Stefan Schwindt (GE Aerospace) 4/25/2024 6:23 AM •
CyberBen
Similar to what Cyrille just showed
http://spoofing.skai-data-services.com/

https://eurocae.sharepoint.com/sites/strato/34fd374d-a1c8-e811-8154-e0071b66a0a1/d07cc886-a856-ed11-bba2-000d3adea767/SitePages/Documents.aspx

Day 5 – 26 April, 2026

Karan restated the rules of the plenary meetings as we are no longer in a working group session and are in a plenary

SG3 status

- Andrew started out
- Reviewed Task Sheet and ToR, key focus on standardized scoring method
- Presented slides on ISMS/ISEM document scope and how to bridge the low-level events (CERT) to the high level scenario (risk-based from ISMS)
- Parsed document and showed mods to ISMS/ISEM interface
- Co-chairs asked for review of the latest draft

SG4 status

- Siobvan started out going over notes for ISMS
- Monday/Wed/Thursday
- Pilot Project lessons learned
- Stefan presented ISMS "big-rocks", only got through risk assessment
- Andrew and Alain presented another view of the integration, pyramid
- Became a Venn diagram where ISEM is almost entirely in ISMS, sliver is airworthiness
- Finally covered steps and needs
    - Key point of asking for presentations
    - Also need to consider small organizations
    - Need to take care of blank sections and either add content or remove the section

SG5 status

- Olivia start out
- Resolved Part IS concerns
- Document will stay harmonized
- Will include a framework in addition to existing use cases
- New EUROCAE Co-chair is Alessandro Oteri and Anup is the new secretary
- Vote at June Plenary to go to FRAC/OC

SG6 status

- Stefan started out
- Resolved non-concur's
- Boeing RB to address communication, navigation and surveillance services managed by national agencies
- Working to resolve remaining comments by June Plenary
- CyberBen is working on getting all the topics needed to be captured in the FAQ

ICAO WGs

- Jean Paul started us out
- New study group in ICAO underneath the Unlawful Interference Committee for information security
- Issue is that there is no documentation that helps ICAO solve these issues
- They want to take advantage of the RTCA/EUROCAE work
    - But ICAO is state driven
    - No one from the committee can attend from their company
    - Only ICCA can attend, and they can only have one person attend and speak
        - Can have 8 advisors, but cannot speak

- Stefan sent out an email with documentation from ICAO with expectation related to Part-IS (ISMS) and event management

TOR

- Siobvan began presenting the TOR
- Change of dates for DO-326B due to change for release
    - Moved from March 2024 to June 2024
- For DO-XXX (ISMS) change of date as well
    - Moved from June 2024 to December 2024
- DO-392A is moved to December 2024
- DO-YYY (DSEC) has been moved to March 2025
- New report for Supporting Information for DO-356A
    - Due March 2025
    - Will not go through FRAC
    - Inputs to "Supporting information for DO-356A" still accepted via faq@cyberben.eu
    the list of topics for DO-356A/ED-203A and in which document will be covered based on our current understanding: https://eurocae.sharepoint.com/:w:/r/sites/strato/8F4CAE54-24D4-E611-80F2-5065F38BC5A1/9435b696-ad71-ee11-8179-000d3ab4bcd9/Meeting%20documents/Options%20for%20DO-356%20ED-203%20FAQ%20companion%20doc.docx?d=w5e822818735b41108bddd592bdbd7bf2&csf=1&web=1

- New DO-356A Change 1
    - Due June 2025
- New DO-355B Revision
    - Due December 2026

Coordination with other groups

- SC-236/WG-96 Wireless Avionics Intra-Communication (WAIC)
    - Issue with comment resolution and issues with Telecom organizations
- AI/ML
    - FAA Roadmap meeting in March
- HSIN ACI COI Access Request Template — Send populated request template to Scott Woodbury
  (scott.r.woodbury@faa.gov):
  •First Name:
  •Last Name:
  •Work email address:
  •What subsite/working group do you want to join: HSIN ACI COI site and subsites
  Reason for joining subsite/working group: ACI COI member
  Sponsor name and email address: ACI COI Host, Scott Woodbury (scott.r.woodbury@faa.gov):
-

S-18

- Ian Coaker started his presentation showing the draft of AIR8480 that is going to show how the system and security processes all work together

ECSCG

USACCESS

- Siobvan present work being done with the USACCESS group

A-ISAC/A4A

- 7/17-7/19 2QAvTech hosted by Lufthansa in Germany
- 3QAvTech 9/16-9/17 in New Orleans, LA
- Aviation Cybersecurity Summit 9/17-9/19 in New Orleans
    - Registration is now open

Next meeting dates

- 2025
    - March 24-28 at EASA HQ in Cologne, GER
    - June 9-13 at Boeing in Seattle, WA
    - September 22-26 at TBD in EU
    - December 8-12 at Southwest in Dallas

Closing remarks