## EUROCAE WG-72 Plenary Meeting #59 / RTCA SC-216 Plenary Meeting #49 "Aeronautical Systems Security"

| Date | 18ᵗʰ September 2020 |
|---|---|
| Place | Virtual Meeting |
| Venue | |
| Hosted by | EUROCAE |

**Attendance:** (snapshot of WebEx attendee list)

| Initial | Attendee | Organisation | Attendance |
|---|---|---|---|
| | Peter McNeeley | ACA (Astronautics Corporation of America) | W |
| | Daiga Dege | ACI Europe | W |
| JGD | Judical Gros-Desire | AIRBUS SAS | W |
| | Brian Hoffman | ALPA | W |
| | Aaron Renshaw | American Airlines | W |
| | Rosemberg Silva | ANAC Brazil | W |
| | Mohammed Waheed | Aviage systems | W |
| | Mark J Kelley | AVISTA | W |
| CDG | Clive Goodchild | BAE Systems | W |
| | Caroline Prado | Boeing | W |
| | Siobvan Nyikos | Boeing | W |
| | Laurent Leonardon | Collins Aerospace | W |
| | Philippe Marquis | Dassault | W |
| TP | Ted Patmore | Delta Airlines | W |
| CR | Cyrille Rosay (Chair WG-72) | EASA | W |
| JPM | Jean-Paul Moreaux | EASA | W |
| | Juan Anton | EASA | W |
| | Claudio Henrique de Castro | Embraer | W |
| | Poliana de Moraes | Embraer | W |
| | Andrew Kornecki | Embry Riddle Aeronautical University | W |
| AG | Anna Guegan | EUROCAE | W |
| KL | Kristof Lamont | Eurocontrol | W |
| | Hannes Alparian | European Defence Agency (EDA) | W |
| | John vanHoudt | FAA | W |
| | Marcus Labay | FAA | W |

| | | | |
|---|---|---|---|
| CG | Cesar Gomez | Federal Aviation Administration | W |
| | John Flores | Federal Aviation Administration | W |
| | Markus Labay | Federal Aviation Administration | W |
| VK | Varun Khanna | Federal Aviation Administration | W |
| | Mitch Trope | Garmin | W |
| DP | David Pierce Chair SC-216) | GE Aviation | W |
| SS | Stefan Schwindt | GE Aviation Systems UK | W |
| | Andy Boff | Helios | W |
| | Sam Masri | Honeywell | W |
| | Manon Gaudet | IATA | W |
| | Mariusz Pyzynski | IATA | W |
| JA | John Angermayer | Mitre | W |
| | Charles Sheehe | NASA | W |
| | Phillip Watson | Panasonic Avionics | W |
| | Philippe Robert | PMV Engineering | W |
| KH | Karan Hofmann | RTCA | W |
| | Cristian Haury | Safran | W |
| | Cyrille Aubergier | SITA ON AIR | W |
| | Kevin Meir | Textron aviation | W |
| | Frederique Dauvillaire | Thales Group | W |
| | Raoufou Ganiou | Transport Canada | W |
| CT | Casey Theisen | United  Airlines | W |
| | Eric Mok | Universal Avionics | W |

**Welcome and Tour de table**

Introductions and tour de table conducted. The RTCA and EUROCAE IPR and Policy statements were displayed and read through by Karan Hofman and Anna Guegan which were accepted by the participants and recorded in these minutes.

**EASA update on Part-AIS (EASA)**

An update was given by Juan Anton of where EASA are with the rule making task RMT.0720 Management of Information security Risks.  The most recent meeting of the ECP (European Strategic Coordination Platform) was held virtually on the 30th September. Timeline for issuing the opinion will largely depend on the maturity of the AMC before issuing the opinion. Have initiated a survey to the ECSP and how the task should proceed. ECSP meetings will be scheduled Oct/Nov Jan. The Option recommended by EASA is the second one where the option is expected around March 2021. See calendar below



## Expected calendar

→ **The most recent meeting of the ESCP (European Strategic Coordination Platform) was held virtually on 30th June/1st July 2020.**

→ **14th September 2020: EASA submitted to the ESCP the following** (deadline for comments on 2nd October 2020):
  → Minutes of the last ESCP meeting
  → New draft of the proposed rule trying to address the issues raised.
  → A survey with some key questions that may impact the delivery time of the Opinion (in particular, one regarding how mature should be the AMC material before issuing the Opinion)

→ **Timeline for issuing the Opinion: Will largely depend on the maturity of AMC required before issuing the Opinion. In particular:**

  → **Opinion expected around January 2021** if Opinion is published before any mature AMC is produced, with a mature draft of AMC to be provided to the EASA Committee before a vote takes place on the rule.

  → **Opinion expected around March 2021** if "Objectives & Implementation Criteria" for the different requirements, instead of producing them as AMC material, they are also introduced in the proposed rule for mandatory compliance (they would be part of the Opinion). Other AMC material, with examples of means of compliance on how to comply with those "Objectives & Implementation Criteria" would be delivered at a later stage. **THIS IS THE OPTION RECOMMENDED BY EASA.**

  → **Opinion expected 4th Quarter 2021** if all the AMC material must be available before issuing the Opinion.

SS – Do you want to discuss any of the other changes in the latest draft and how that will impact our standard activities.

JA doesn't think they will impact, they have changed the structure concerning management of risk and reporting, and providing the requirements in a more logical sequence. These will have objective included in the rule, standards will be referred to in the rule.

CDG how organisation outside will be affected and MRO's that are third countries.
JP said that the rule will not affect outside orgs.  It is limited to European manufacturers but they may apply to European owned orgs outside Europe.

VR. FAA is in the process of developing Part 25 rules. The question on the impact on non European organisations has also been raised at the ECSP by FAA and whilst it should be limited to European operations. There still needs to be some work as there are some open questions in this area

CG – raise three questions:
1.   Operational ramifications of US operators working in Europe including drone operators.
2.   US Part 23/25/27/29 Manufacturers and TC/STC product holders though covered by the current bilateral agreement from meeting the requirements of the rule. Being suppliers of products to European markets what is levied on their organization from the Rule requirements.
3.   European Manufacturer that has a US facility, are they expected to comply with EASA organization rules in their US facility? Would the FAA have to conduct oversight of an

organization and/or repair station on EASA's behalf for the organization cyber security requirements?

JPM The third one is correct the other questions need to be addressed. The rules will apply to contractors to European companies

VK – FAA is in the process of developing Part 25 rules. The question on the impact on non European organisations has also been raised at the ECSP by FAA and whilst it should be limited to European operations. There still needs to be some work as there are some open questions in this area There is a need to understand the perimeter of the rule and need the clarification so issues understood

CR presented an overview around decision 2020-06/R: products, doesn't cover unmanned yet
- New AMC20-42 Airworthiness information security risk assessment
- Under development is ASTM F44, for small airplanes
- Applicability is January 2021
    - Legacy aircraft no change unless it is significant from a Part 21 point of view
    - New type certificates



## Products – impacted regulatory material

CSs and associated AMCs
→ AMC 23.2510
→ CS 25.1319 & H25.6
→ CS 27.1319 & A27.5
→ CS 29.1319 & A29.5
→ CS E.20 & E.25
→ CS P.230 & P.40
→ CS APU.90 & APU.30
→ CS ETSO A.2.6

New AMC 20-42
Airworthiness information security risk assessment

Existing standards
(EUROCAE/RTCA)
ED 202A-DO 326A
ED 203A-DO 355A
ED 204-DO 356

(under development ASTM F44, for small airplanes)

CG will slides be available for download – CR yes

PM requested clarification on what a significant change is

SS – Raised that industry needed was clarification on what was is a significant change, and raised glass cockpit as example
- Can a change be significant because of cybersecurity impacts of the change?
- What is considered as affected area in case of a significant change from a cybersecurity point of view?

CR Minor and major was discussed, even if not a significant change, the applicant will use the legacy certification basis augmented by a Special Condition.

SS – If we change interfaces that introduce new attack surfaces then yes, but if it was a purely mechanical change that was major. We could do with guidance on what is an significant change with respect to security.

CR
Proposed that the industry could come with a white paper on information security elements that could trigger a change to be major/significant.

- Action white Paper from industry

Post meeting: Clarification on the topic: it is part 21.A.101, also known as the "change product rule".

**SG2 Coordination (Kristof)**

Kristof gave an overview of ED205A kick off meeting and schedule
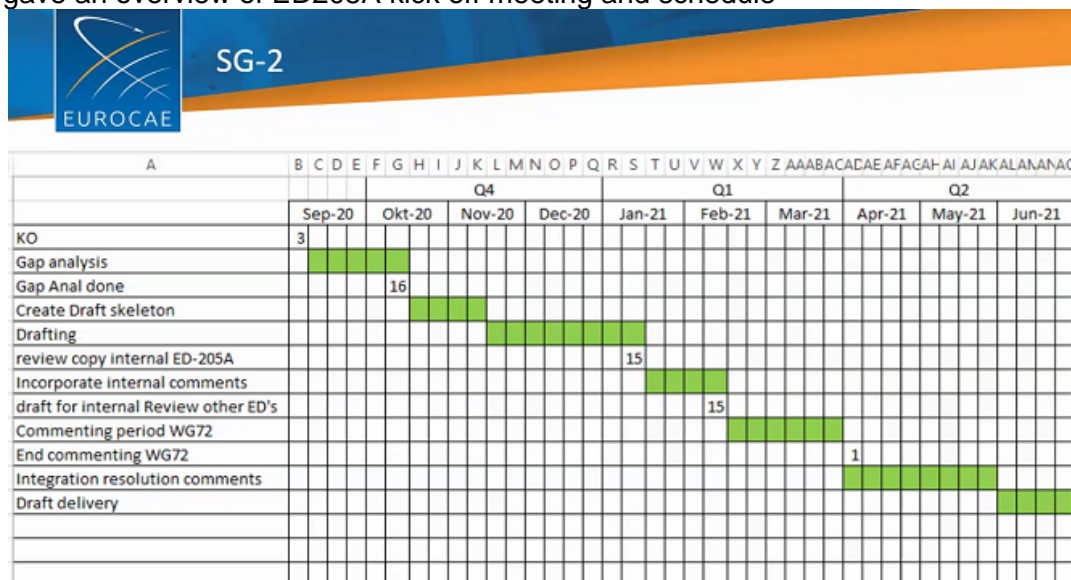


- Andy Boff is currently the interim secretary and Jerry Hancock will be the industry editor
- The main point from kick-off meeting is the review of the existing material (e.g ED series) to see what has been done
- Aiming for a draft of the document by the end of Q2 2021
- Important that we have a discussion with SG-4 to ensure as minimal overlap as possible and the documents are complementary. This includes consideration of ground system and harmony b/w ED-205A and ED-201A
  - See action in SG4 report
- CR – need to discuss the timescales and whether scope should be reduced to meet the rule timescales
- DP – raised that there are discussions on whether SC-216 should also pick up this document. If SC-216 think this is important then contact DP or VK
- VK – From the 216 it is currently out of scope and there is not much enthusiasm to expand the charter, but appreciate harmonised is preferred, but some traction in the agencies is required as SC-216 is primarily aircraft centric. He pointed out that there is a benefit in harmonization between Europe and the us but that there is still work to be done to ensure harmonization.
- CDG raised ED205A needs to take into account the comment sheet and resolutions
- KL to inform the group

Break 15 minutes

**SG3 (Judicael)**
Frederique gave an overview of the progress of SG3
- ED204A/ED355A is now published

**ED-204A Status**
⇨ See slides for location of document and final comments status.
⇨ Publication Done  after official approval by Eurocae and RTCA
  ✈ Slide status ED-204A DP et official Via: SG-3 subgroup /document project /  ED-204A , URL => ED-204A DP

- CR/VK/DP congratulations and gave thanks to all those involved, and especially the editors
- ED-XXX (ISEM) progress – issues- timeline

- o The table of contents is now stable but there will be more discussions on some of the remaining blocking points with a target of a draft by the end of the year
- o All comments now need to be provided in a more formal way, so from next draft onwards comment sheet



- o Yesterday had presentations from two airlines and Eurocontrol, this was good to see examples of practices that have been put in place, and takeaways from the presented will be considered. Also agree a way to complement the safety occurrence reporting process, so discussion can go forward with the safety committee
- o JGD The presentations showed we are covering the areas so valuable.
- o FD presented the revised schedule, open consultation March 2021, Target date for publication Q3 2021.

Actual Status as per approved TOR (Eurocae / RTCA)

o So first critical milestone is to have a mature draft produced by the end of this year. Which will mean compilation by the editors of all existing material in one word document starting Oct 2020.
o DP raised that he is going to request a six month change to the PMC
o JDG – So we need a stable draft and inputs from other domains



✈ Having a draft mature for Dec 2020 session (last word is from Nov 2019)

✈ Based on discussion, here status by chapters

| Chapter ref. | Main open points | Maturity/readiness |
|---|---|---|
| 1-Introduction | | Mature |
| 2-Process | Safety Occurrence Reporting versus Security Reporting to be adopted | Mature |
| 3-Organise & Process | Scoring in general and vulnerability management | Not Mature |
| 4-Detect | Too a/c centric and dilema real time /post incident anlysis | Not Mature |
| 5-Analysis | Adjustement with chapt 3 & 4 , more concrete workflow /triage needed | Not Mature |
| 6-Respond | ?? To do | Mature |
| 7-Recover | Debate with VDP and Information shaing in chap3 | Mature |

o FD – Chapters 3, 4 and 5 are not mature or agreement is required. 1,2 6 and 7 are mature
  ▪ Chapter 3 scoring in general and vulnerability management
  ▪ Chapter 4 too focused on the aircraft
  ▪ Chapter 5 needs adjustment with chapter 3 and 4
o TP – Do we have everything to build the document
o The way forward will be workshops every 3 weeks and then once the chapters have been reviewed and the main points are resolved produce the full document
  ▪ Chapter 3 [1h30 or 2h]
o Dedicated workshop about scoring based on an exercise Vulnerability management : scoring option (CVSS standard is preferred, feedback from Airbus which incorporated Safety aspect)
o Vulnerability Disclosure program to detect by an external reporter a potential security incident /event / Vulnerability.
  ▪ Chapter 4 [1h30 or 2h]
    • Need to move away from A/C centric more Aviation eco system.
    • Focusing on list of events of interests as per standards ( aviation, security)
    • onboard multiple contexts : log available or not, real time analysis or not
  ▪ Chapter 5 [1h30 or 2h]
    • Need to focus to define the steps to proceed to analysis, focusing on confirmation or not of incident.
    • Define timeline, threshold as per scoring from chapter 3 etc
    • Adopt a short time remediation strategy (Respond)
  ▪ Review chapter by chapter once main points are resolved + full doc review

at the end
- ▪ DECISION: The plan is to have a full draft of the document completed by December


**SG4 Report (Stefan)**

- Stefan gave an overview of the progress  and the schedule for ED201A



- The validation exercise was conducted in March and SC-216 has joined the document. A chapter by chapter review has been conducted over the summer period
- We have addressed all the NC comments and 67 of the H comments
- Way forward
    - o Need to get classification for unclassified comments
    - o Make a new request for chapter 4 and 5
    - o Schedule meetings to resolve any new H and NC comments
    - o Section leaders will engage with the M and I comments
    - o We need to update scope to account for organisations
    - o Need to synchronise content with ED-ISEM and ED205A
    - o Then re-issue draft, create examples , perform validation exercise
- CR highlighted that the validation exercise in Madrid 5<sup>th</sup> and 6<sup>th</sup> March) was a joint WG-72-SG4 and ESCP exercise
- ToR indicate we should already be in open consultation, chapter review has impacted the schedule, plus with ED205 starting we introduce a shift to ensure align we the other documents
- Draft 2020 Revised draft with comments resolved
- Validation exercise January 2021
- Open Consultation/FRAC March 2021
- Complete resolution June
- Ready for PMC September 2021
- Location for ISEM content
    - o Section 3 currently has objective for ISMS
    - o Full ISMS would significantly increase size of ED201A
    - o No other standard is in development – so should a new activity be initiated
- CR This could be discussed in ECSCG  new standard or ED-201A
- SS not all elements in ED201A so new standard whether EUROCAE/NIST or another
- CR – Point has been taken
- Action
    - o SG4 to arrange a meeting to review and agree the scope of what should be included on the ISMS for ED201A and whether there should be a new standard and what the scope should be
    - o Material then to be removed from ED201A to be included in a stand alone whitepaper for future use
    - o Provide the proposal of a new standard if required to the ECSCG
- DP raised the comment that SC-216 is not part of 205 so need to be careful with the references
- SS proposed adding a footnote in ED201 to clarify if SC216 does not use ED205.
- VK said that this item needs to be discussed and presented to the FAA.  He added that

the FAA may decide in favour of expanding RTCA SC 216 TOR.

- KL – raised is the use of an ISMS really new
- PM – We should provide all the detail for an ISMS but should focus on what is required for our domain, and what is needed to understand is what AMC material is required to support the Part-AIS
- SS – This is a challenge as there are standards out there but what are the add ons required for Aviation, and is objectively measurable
- CR proposed a reduced text is just kept in ED201A and we put the action on the ECSCG
- PM So for the compliance material we currently have, so we remove or keep
- CR we probably need a separate discussion in ED201A
  - o Action have a separate meeting on ISMS involving ED205A
- SS Other synchronisation with ED205A is the overview of Security (Assurance) Level for mapping and description for the mapping
- SS For Synchronisation ED-ISEM location of the incident response overview and information sharing guidance
- FD We need to decide and co-ordinate on this content
- SS Need to define and agree the scope of information sharing
- SS We don't discuss commercial in ED201A and incident which should be in ISEM
- CR we need another dedicated meeting for this, what is the schedule
- SS These meetings need to be scheduled
- FD requested where these points have occurred
  - o <u>ACTION SG 4 to create these meetings to organize by SG-4 a meeting to resolve conflicts B/W ED-201A with other documents (ISEM, ED-205A .)</u>


Break

**ER-13 (Clive)**

- Clive gave an overview of the document status



- AG the edits need to be done and then we need a peer review of the document for a couple of weeks before publication
- KH – RTCA are still working how they can publicise this, so if AG sends the document and then RTCA can then see how they can take forward and how it can be approved
- 

<u>**Liaison with other working groups (Cyrille)**</u>

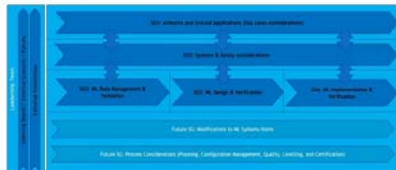Cyrille led the discussion on the liaisons with other working groups

WG-114 on AI (joint with SAE G-34)

- Clive gave an update of the group activities and where WG-72 involvement will primarily be to highlight gaps



- Typo with SAE 216 to RTCA 216, also ED204A is not being correctly referenced – this needs to be added to the comment sheet

SAE G-32 Cyber Physical Systems Security Committee

- Stefan Schwindt gave an overview of SAE G-32 and committee members have been directed not to duplicate ED20X series, However they are developing complementary material that may be useful
  - E.g testing metrics – stop criteria



-

WG106 – EFB (and the closed OC on ED-273 which incorporated as a proposal security requirements not aligned with WG72 standards …)

WG-98 SG-1 (Return link Service of Emergency locator transmitter):

- Risk assessment on the end to end system (Cyrille)
- Could potentially be a use case for ED201A

WG105 UAS / RTCA SC-228
- Nobody knows the status, we need a liaison and coordination with this group

WG112 VTOL
- SG3 – Safety responsible of cybersecurity (Cyrille)
- May have an impact on ED203A which may need to be re-opened

SAE E-36 committee (engine Control systems)
- SS presented the SAE E-16 Status
- Due to COVID, the committee did not have the minimum numbers to convene, interested parties can join
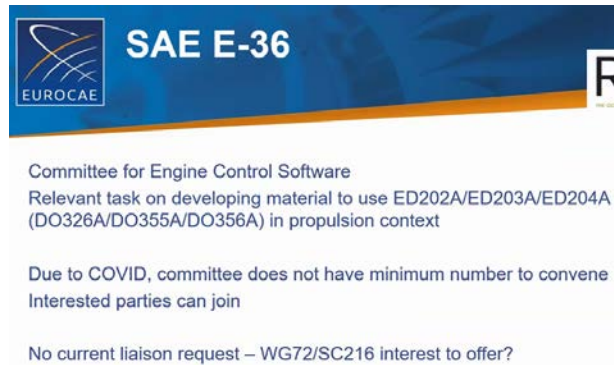


-
- SS – The group is now live, but EASA is not on the link

It is proposed that WG72 chairman Cyrille (or leaders as backup) will dedicated a quarterly meeting to present on going WG72 work and synchronize with others WGs . In formation security will be the first topic
- Action is in place to progress this
- AG –There is a new platform for leaderships so there is an email to reach all the leadership and will be a location for the first cybersecurity meeting
- 2 hour webex agreed to check with the other working groups

CT raised SC-224 Airport Security Access Control Systems

ECSCG report and next meeting
- AG Next meeting will be the 8th October, a request to everybody to respond to the questionnaire, deadline 1st October

## **AOB and Next Meetings (All)**

DP – There is a revised TOR he would like to discuss and review with SC-216. Any comments or questions or disagreements with the changes.
- CDG raised ER-13 will be ER13A
- SS Raised how will you handle ED205,
- KH stated we might be able to do an electronic approval if that can be done by December 17th
- SS Change title to Information Security event Management
- Agreed and will be presented at the next PMC

Date of next meeting
- A doodle will be arranged to confirm the following dates that was discussed at the meeting

| | |
|---|---|
| December 7-11, 2020 | DO-xxx/EDxxx FRAC/OC Disposition Meeting (Virtual, Hosted by RTCA) Timeframe: 9 – 2PM eastern |
| March 15-19, 2021 – (doodle) | Virtual – (hosted by EUROCAE) |
| June 7 to 11, 2021 – (doodle) | BXL – Paris? |
| Sept 13-17, 2021 | DC? |