



EUR 086/19 WG72-124
RTCA 093-19/SC216-091

Saint-Denis and Washington, 22 March 2019

EUROCAE WG-72 Plenary Meeting 53 / SC-216 Plenary 42

Date	22 March 2019
Place	Paris
Venue	23 rue Paul Lafargue, Saint Denis, Paris
Hosted by	EUROCAE

Attendance:

Organisation	First name	Last name	19-20	21	22
Airbus	Judicael	Gros-Désir	X	X	X
Airbus	Gilles	Tehel		X	
AKKA	Philippe	Robert		W	W
ALPA	Brian	Hoffman		X	X
BAE	Clive	Goodchild	X	X	X
Boeing	Siobvan	Nyikos	X	X	X
CAA/SRG	Peter	Davis	X	X	X
Collins	Laurent	Leonardon		X	X
Dassault	Philippe	Marquis	X	X	X
Delta	Ted	Patmore		X	X
EASA	Cyrille	Rosay		X	X
EDA	Hannes	Alparslan	X	X	
Embraer	Claudio		X	X	X
Eurocontrol	Kristof	Lamont			X
Eurocontrol	Aleksandar	Momiroski		X	X
Eurocontrol	Timo	<i>Blunck</i>	X		
FAA	John	Flores	W	W	W
FAA	Varun	Khanna	X	X	X
F-Secure	Benjamin	Nagel	X	X	X
GE	Stefan	Schwindt	X	X	X
Helios	Andy	Boff	X		
Honeywell	Sam	Masri	X	X	X
IATA	Sergio	Fernandez		X	
IATA	Stefano	Prola		X	
IATA-Qantas	Tim	Cooper	W		

IATA-KLM	Herman	Verhoef	X		X
Inmarsat	Jerry	Hancock	W	W	
Lufthansa Technik	Kai Florian	Tschakert		X	X
Panasonic	Philip	Watson	X		X
Safran	Christian	Haury		X	
Teledyne	Ravi	Nori	X	X	X
Thales	Frederique	Dauvillere		W	
Thales	Gilles	Descargues	X		
Thales	Cyrille	Marchand		X	X
Canada Force	Marek	Hrubesz		W	

Additionally Referenced Individuals

1. Welcome
 - a. Introductions – tour de table
2. PART –AISS
 - a. Eric Vautier
 - i. Associate of European airports, participates in EASA ESCP
 - ii. Talking about EASA regulations and how it pertains to airports
 - iii. Airport Council International = ACI in this case
 - iv. ACI is joining WG-72
 - v. “The Cyber Airport” guide released
 - vi. Brought up NIS directive, it is for protecting critical infrastructure (which includes airports), important for information security in Europe
 - vii. Each country determines how to transpose NIS directive
 - viii. Also showed EASA high level operational plan (i.e. roadmap)
 - b. Around the room comments on pr3senations
 - c. SN – I’m familiar with European regulations, good presentation, good to have airports involved as they are part of aviation ecosystem and end-to-end security
 - d. JD- Taking assumptions on what needs to done at the airport is done, and the airport is a key part of the chain.
 - e. EG: As an airport would like to know what assumptions are actually made by Airbus as he is unaware. Airline can upgrade the aircraft and airport does not know what the security assumptions were made on any connections and what the duties of the airport are.
 - f. BH Do you see the same controls for passengers and cargo. Cargo is a specific world and needs to be addressed
 - g. CM – Good news that ACI is joining EUROCAE, want to participate and understand each other, will help in generating examples for event management, more stakeholders the better
 - h. PM, BN Echos Thales comments
 - i. PD – Intrigued to hear about NIS and Part-AISS compliance, at the moment what is being proposed is a disaster as NIS is nation and Part-AISS needs to be consistent. EN1695 is out of date as it does not reflect the new 27002. Assumptions
 - j. SS – NIS direction has already happened, and people want NIS directive as an AMC but a NIS coordination group may improve matter.
 - k. EG – Really waiting for someone to say what systems need to be cybersecure
 - l. PD – UK Guidance and tool is on the NCSC website, and one of the key questions what are the critical systems. NCSC can say what critical functions and airport needs to determine what are the critical systems.
 - m. EG – Question of interpretation some UK airports may say if my screening equipment is hacked its nothing to do with the NIS directive. It is going to be a continuous improvement process. We need to understand which functions are critical
 - n. STORM and ED-201 are working this too, want airports to contribute to ED-201
 - o. SS brought up NIS directive again, Eric said best countries will drive the others
 - p. PW – often airports are weak link in the chain, glad ACI is here to strengthen that
 - q. JD – would like ACI participation on ED-xxx as well
3. EUROCAE/RTCA Participation in the working groups
 - a. Anna gave a summary presentation of EUROCAE and Working Groups functioning process
 - b. Siobvan provided some opening remarks for RTCA
4. SG-4 – SG Chair gave the following overview

- a. PD gave an overview of the meetings held this week, concerning the update of ED201, partly to take into account the newer ED documents, improve coverage of the content.
 - b. Discussions at the meeting focused around the external agreement
 - c. Relationship with ED-XXX ED201 will cover incident and vulnerability at sharing/reporting at a high level
 - d. We will remove the word civil out, so document could then be applied in military context
 - e. Discussion around whether ED201 applies only to operational situations or it also applies to product development, will cover both and the difference will need to be explicit in the document
 - f. ECSP STORM – ED201 will turn outputs from STORM into guidance, Need STORM to validate the approach of ED201, CR will clarify how people can support STORM.
 - g. Face to face meetings in June and September and November with periodic webex
 - h. Dependent on inputs from STORM, taking STORM inputs and putting into guidance/standards
 - i. April 16-17 in Brussels - next STORM meeting. How to get STORM to participate, need agreed tasks at the next meeting
 - j. As for SG-4, next meetings June, September, and November, aiming for Open Consultation (OC) in 2020
 - k. Around the table
 - l. SN – even though RTCA is not participating in SG-4 activity, Boeing is a full member of EUROCAE and will participate as much as we are able
 - m. SS brought up AMC and dependencies
 - n. It would be good to get more stakeholders, good to have Eric onboard for airport perspective, good to have EUROCONTROL and airlines participation as well
 - o. PM – Would expect some guidance on governance and classification of information – high level and principals, and an extra level in the external agreement. TLP is one method for handling, but for data handling - there is National classifications, export classifications.
 - p. CG – Can only keep this at a high level and principles else we will stray into legal and lawyer territory
 - q. National security data doesn't fit with Traffic Light Protocol (TLP)
 - r. PM – Need to keep ED201A and EDXXX aligned, may need to calendars aligned
 - s. Philippe wants to synchronize schedules of the subgroups as there are more links than we thought between ED-201A and ED-xxx
 - t. Stefan – pace of ED-xxx will not support ED-201A schedule, divvy up by chapters?
5. SG-2 Report – SG Chair
- a. KL gave an overview of the SG2 activities concerning the ED205 document
 - b. Waiting on the publication of the document – currently a process specification for certification/declaration, lots of comments that more information is required. Do we reiterate ED205 or come up with a new EDXXX which would meet the new regulation and outputs from STORM
 - c. Current document touches on the steps in the document, but does not consider what methods need to be used as an acceptable means of compliance
 - d. SS –nPart-AISS covers the organisation side, are there systems certified/accredited directly and systems certified/credited under Part-AISSs.
 - e. KL: There is currently no regulation currently to certify the ground systems. In some states they say you can only certify the organisation and not the system and some disagree. What is needed is the certification of the whole system. We want to be ahead of game and parallel with EASA ESCP
 - f. Process and method as two separate documents, but you need to avoid another set of documents for the support systems
 - g. KL – The problem is that certification does not mean the same across all the stakeholders
 - h. CR – Certification of service provider has stalled a little, CR will look to get some feedback on the status of this, and there may be an equivalent gap with the service providers in the airport. How do we take account the service information providers
 - i. CR Raised INNOVA
 - j. SS – This is partly risk sharing – STORM, link between 202 and 205 can be done in ED201A,
 - k. PD – We could include considered risk assessment methods in an annex and whether they are comparable. The other topic is how
 - l. Assurance is one area, and the outputs of the assessment, plus the method you used
 - m. CR Do we need to connect the methods,
 - n. We have two areas Trust Framework around organisations and the we also have areas like SWIM who provides the information where in the nodes
 - o. Kristoff – not sure how Innova will be implemented but should be trust between ground and airborne part based on a certain level

- p. Identity management – how do you know it's really that person on the swim network?
 - q. CR. – mitigate to acceptable level, why can't you harmonize what those levels are for ground and airborne?
 - r. KL – up to organization what risks and how they want to mitigate, org A in member state A is not going to do the same as B, even though they use same methods, subjectivity in likelihood
 - s. External factors of countries may be different
 - t. Comparison shouldn't start with methods, what's important is the outputs/outcomes
 - u. Different risk appetites in different organizations
 - v. Translation table of methods from STORM (need to be careful about sharing, keep to within EUROCAE)
 - i. Post meeting note, the principal should be that the granularity should be enough to identify large mismatches of risk between connected organisation
6. Lunch
7. SG-3 Report – SG Chair
- a. JGD – Reminder of the agenda of 21st, March 2019:
 - i. Basics
 - ii. What
 - iii. How
 - b. JGD - Summary of achieved/incomplete topics discussed by SG-3:
 - i. Key Action 1: Definition harmonization between SC-216 / WG-72
 - ii. Key Action 2: Inputs for ED-XXX creation needed by SC-216/WG-72 members, any format accepted (e.g examples/diagrams/text/etc...)
Key Action 3: ED-XXX content creation (first proposal provided by BOEING)
 - c. Unclear way forward on ED204A, no formal agreement on the proposed topics to be included/removed from ED204A.
 - d. JGD – Unclear way forward partially agreed, since no subgroups have been created to draw the first sketch of ED-XXX chapters; Key Action 2 only partially answers to the way forward by working on example scenarios for security event management.
 - e. Try to do biweekly webex before June meeting
 - f. DP when those comments were generated, we had no notion of event management doc, those comments will be absorbed and addressed
 - g. KL – Scope of ED-XXX extends to ground systems; synchronization is needed with ED205 WG72 Subgroup
 - h. SS – ED204A: Scope aircraft + ground systems attached to aircraft, also need to be synchronized with other subgroups. needs to include scope of Part-AISS as well (to include airports)
 - i. PW – “Branding” is added to the scope of ED-XXX on presented slides, but not discussed on 21st March meeting -> SS/JGD: Branding was mentioned in the flow chart of Security Event Management Process, but not discussed. The aim was to highlight “non-safety security incident” that could have other impact on operation or branding and could be worth being shared on voluntary basis.
 - j. Way Forward for ED-XXX: additional examples could involve ground systems to show how Security event management may impact the overall aviation domain. Example should show how communication is established between key stakeholders to be able to respond to security incidents and report those with safety impact to airworthiness authorities
 - k. BH – How to manage events / incidents detected in-flight by crew?
 - i. SS – typical cases should be illustrated by the group
 - ii. JGD – Information provided to the crew in-flight during a threat attack has been discussed previously, past studies showed that current procedures and messages systems are sufficient; this topic might be out of scope of ED-XXX; current scope would be pre-flight/post-flight phases.
 - iii. CR – several examples exist based on EASA studies; outcome of the example is that current EICAS messages and procedures are enough (e.g. database hacking, ...). Moreover, several studies have shown that erroneous information to the pilot are detected by the crew and considered as temporary error of the system; in those cases, appropriate actions have been taken into account.
 - iv. VK – Currently, a system failure leads to an EICAS message; in case of a cyber event, same process would occur, if system integrity is affected.
 - v. BH – There is a concern in case of cascading failures due to a propagating attack, pilots should be aware of what is happening and of the correct action to take.
 - vi. VK – This would involve a new set of dedicated messages due to cybersecurity events that would stress the cabin crew or the pilots; if the attack ends up by the

failure of a system, current process and EICAS messages would apply, so no need to add new type of information for the crew.

- vii. SS – restates that such example should still be developed by the group to understand the consequences of such event; the group will then be able to capture this case or disregard it.
 - viii. VK – Another point raised is the current technical difficulty to differentiate a system attack from a system failure during flight.
- I. Next face-to-face meeting in June 2019, Washington DC

8. General

a. RTCA

- i. SN – ED201A – RTCA may have to think about the content of this document and how it makes sense to incorporate its content in its documentation.
- ii. SN - Regarding definition for ED-XXX on vulnerability, security events & incidents, there should be no strong disagreement among the group members
- iii. VK – great decision that RTCA joints EUROCAE work on the updates of the standards
- iv. SS – ED201A should be recognized into A(M)C at some point to align applicants on a common framework for security aspects.
- v. CR – ED201A may not be mentioned, the AMC content will glue the other standards altogether

b. SG Harmonisation – any Issues

- i. SG2: ED205 – How to tackle issue with the future ED205A/ED20x? A new TAC will suggest the addition of a supplement for methodology and proposed to the executive committee. Current scope is limited to WG-72. RTCA position could be helpful.
- ii. No strong concern from the members in the meeting; however SS remarks that releasing 2 documents might raise harmonization issues between ED202A/ED203A and ED205A/ED206 by comparing the 2 sets altogether.

c. Schedule and way forward

- i. Next meeting is planned on week 10th/14th June, 2019
- ii. Aviation ISAC is planned on October 28th to 1st November, 2019
- iii. Next RTCA/EUROCAE joint meeting could be planned either before or after the Aviation ISAC meeting:
 - 1. proposed on 21st/25th October,
 - 2. Thursday 24th planned to be a plenary meeting for SC-216/WG-72
 - 3. *This meeting would be the decision for FRAC / Open Consultation for ED204A/DO355A*
- iv. Intermediate webex/telecon planned between face to face meetings, see slides provided by Dave P. "SC-216/WG-72 Proposed Schedule"
- v. Proposal for an intermediate face to face meeting in EASA or Eurocontrol in Brussels on the first week of September -> to be confirmed asap for availability of conference rooms (& hotels in Brussels)

9. AOB

10. Close