EUR: 190-20 / WG72-142
RTCA Paper No. 254-20/SC216-111 Saint-Denis and Washington, 17 September 2020

EUROCAE WG-72 Plenary Meeting #57 / RTCA SC-216 joint Meeting #47

"Aeronautical Systems Security"

Minutes

Date (all sessions)	***Tuesday 2 to Thursday 4 June 2020 - 8AM-12PM EST***
Place	***ONLINE***
Venue	*WEBEX*
Hosted by	***RTCA & EUROCAE***

Attendance:

Contact	Organization
Aaron Renshaw	American Airlines
Adrian Waller	Thales Group
Andrew Kornecki	Embry Riddle University
Anna Guégan	EUROCAE
Benjamin Nagel	F-secure Cyber Security Services Oy
Brian Hoffman	ALPA
Brittany Skelton	The Boeing Company
Casey Theisen	United Airlines
Cesar Gomez	FAA
Chuck Royalty	Aerospace Systems Cyber Security
Clive Goodchild	BAE Systems
Cristian Bertoldi	AIRBUS SAS
Cyrille Rosay	EASA
David Pierce	GE Aviation Systems US
Ed Hahn	ALPA
Ernie Condon	NIAR
Frederique Dauvillaire	Thales Group
Hannes Alparslan	EUROCAE
Jerry Hancock	INMARSAT
Joacy Freitas	ANAC-Brazil

John Angemayer	The MITRE Corporation
John Flores	FAA
Judicael Gros-Desirs	AIRBUS SAS
Kai Florian Tschakert	Lufthansa Technik AG
Karan Hofmann	RTCA, Inc
Kevin Thomas	American Airlines
Laurent Leonardon	Collins Aerospace
M. Waheed	Aviage
Mariusz Pyzynski	IATA
Mark J Kelley	AVISTA
Mitch Trope	Garmin
Oliver Palumbo	?
Philip Watson	Panasonic Avionics Corp.
Philippe Marquis	DASSAULT AVIATION
Philippe Robert	PVM-CS
Ravi Nori	Teledyne Controls LLC
Roman Fischer	Skyguide
Sam Masri	Honeywell International
Stefan Schwindt	GE Aviation Systems UK
Ted Patmore	Delta Airlines
Ted Kalthoff	NIAR
Varun Khanna	FAA

02 June WG-72 SG-3 SC-216 (ISEM review by chapter and topics)

Welcome and Introductions

Introductions conducted and were facilitated by David Pierce. Objective was set to work resolutions for the remaining ISEM document comments.

Discussions on the ISEM document started. We will be covering ISEM and ED201 this week. Next week we will discuss ED204 comments and resolutions.

The plan is to have a draft completed by September.

Dave Pierce presented a status summery for chapter 1. A need for clarification of the scope was identified. Phil Robert took the action to write the scope which will include all information systems that have safety impact.

Varun added that we are aircraft centric and that we don't want to manage the whole commercial aviation eco system. Stefan added that this document establishes the guidance for organizations involved in civil aviation activities to identify, protect from, detect, respond to and recover from those information security incidents which could affect aviation safety. Stefan added that we had previously discussed that we want to set objectives for all aviation activities in Security Event plus provide additional specific objectives for sectors as necessary (e.g. for aircraft). Phil M. responded by adding that such scope is too general when compared to other standards dealing with incident managements. He suggested that we should be adding the specific applications into the scope. Ted said that the balance between Aircraft centric and aircraft eco system (off board systems) is the tricky point for this document.

Ted Patmore presented a status summary for Chapter 4.

Phil W. asked for an explanation of how both airworthiness and non-airworthiness events can have safety impacts? Stefan responded that there are more than just an aircraft and safety can be for example, an ATC failure. Ted said that Airworthiness is not the same as aviation safety. Airworthiness refers to the proper flight function of the aircraft. Aviation safety can include systems that affect the process of flying the aircraft. John Flores explained that airworthiness is when an aircraft or one of its component parts meets its type design and is in a condition for safe operation.

Dave P. asked if it is necessary to speak about airworthiness since we are only interested in safety impacts. Stefan responded that we should have safety as a general objective and we can use airworthiness when talking specifically about aircraft.

Philippe said that it is up to each organization to define the list of sources for events to be monitored based on its risk assessment (incident management is considered a security measure)

Judicael agreed and said that Chapter 3 will identify the types of events to monitor and potential means available to reach these objectives, He explained that some items should be part of chapter 3. Chapter 4 seems to compensate.
Distinction AW non AW should be part of chapter 5.

Brian H requested that real time detection of aircraft cyber risk be addressed as a provision for the future. He also asked how we are going to differentiate between real-time vs post event detection. Phil R. added that some tools exist to implement real time intrusion distinction (but not in the aircraft). Judicael proposes to add a section to explain real time detection. However, Judicael said that there may be a need to consider what conditions would possibly require real time detection. Phil M. cautioned against the idea. Phil M. said that different analyses and requirements exist that would determine if an incident is safety related. Ed H. provided suggestions for future real-time objectives for ACD as follows:

Objectives for future real-time: (1) Real-time monitoring of systems in the ACD is an end goal, no different than how real-time monitoring is used in every other domain today. (2) Real time capability should alert the flight crew to safety conditions with an appropriate Airplane Flight Manual procedure to address the safety concerns. (3) Other operational procedures (e.g. MEL, ETOPS, etc.) must also take into consideration that Cyber events are different from simple equipment failures and may require more extensive analysis of the integrity of systems connected to the equipment that is affected.

Philippe R. suggested that real-time monitoring of the aircraft systems should be per the DAH instructions.

Clive mentioned that he made a comment under chapter 5 to have the overall process mapped and chapters and scope aligned. He also added that there needs to be guidelines written around where real time detection objectives are to be implemented

Few slides on ISEM Draft chapter 4 feedback were presented.

Chapter 3 status summary was presented by Cristian Bertoldi.

03 June WG-72 SG-3 SC-216 (continue ISEM))

Today is day 2. Dave stated that our objective today is to work resolution to remaining comments. There are few remaining comments. Grouped by topics.

The day started with a chapter 2 and chapter 5 status summary presentation by Judicael.

Action: Stefan will get back to Ted about a decision to give vulnerability a separate chapter.

On reporting, there was a suggestion to reference safety guidance for reporting incidents that have safety impact. Stefan suggested that there is a need to define thresholds for reporting, both to regulators and through supply chain and it should be based on consistent scoring of vulnerabilities. Phillip W. agreed and mentioned that there will be difficulty is in scoring ground system events. He suggested that we clearly use existing CVSS and then adjust final score by safety impact. Clive suggested that there should be a white paper on vulnerability scoring.

Stefan said that ED201A introduces concept and states that an external agreement RASCI for all activities should be agreed between partners. Here would make sense to suggest that RASCI within an organisation handles activities or the typical RASCI in reporting. John Angermayer agreed.

Varun reminded everyone that the intent was not to change a lot in this document. Everybody agreed to avoid diverging discussions

There was a discussion about means of compliance. It was agreed that it is not the purpose of this document to decide what are the AMC. The regulator is the one who defines AMCs

Sam M. provided a status of Chapter 7, Recovery.

Stefan provided the following: EASA 145.A.25 (d) Secure storage facilities are provided for components, equipment, tools and material. Storage conditions ensure segregation of serviceable components and material from unserviceable aircraft components, material, equipment and tools. The conditions of storage are in accordance with the manufacturer's instructions to prevent deterioration and damage of stored items. Access to storage facilities is restricted to authorized personnel.
FAA 145.103 (2) Facilities for properly performing the maintenance, preventive maintenance, or alterations of articles or the specialized service for which it is rated. Facilities must include the following:
ED-202A / DO-326A and ED-203A / DO-356A provide guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate (Amended Type Certificate, Supplemental Type Certificate and Amended Supplemental Type Certificate) is issued for the aircraft type design. In addition, it includes the handover of information about the Type Design that is necessary to ensure continuing airworthiness with respect to possible information security threats.
ED-204A / DO-355A (this document) provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration and deconstruction. ED204A is for after TC. Specific handling and managing is covered in the documents generated by the DAH in the TC process if applicable as part of the TC process.

There was a general agreement for Stefan's input.

Brian H asked that the preceding discussion on real-time between Brian and the committee be included in the minutes. Dave P. confirmed that it will be.

Remaining comments were reviewed and dispositioned. A comment was made that Ch 5 should be before incident determination,

Judicael suggested that community sharing should occur if it was determined that an event has occurred.

Ted P said that Airworthiness related incidents should require specific recovery processes, like recovery from any other airworthiness related system failure.

04 June WG-72 SG-4 (ED-201A/DO-XYZ)

Contact	Organization
Aaron Renshaw	
Adrian Waller	Thales Group
Alain Combes	
Anna Guégan	EUROCAE
Armella Gauthe	
Benjamin Nagel	F-secure Cyber Security Services Oy
Brian Hoffman	ALPA
Brittany Skelton	The BOEING COMPANY
Casey Theisen	AA

Cesar G	
Chuck	
Claudio H	Embraer
Clive Goodchild	BAE Systems
Cristian Bertoldi	
Cyrille Rosay	EASA
Daiga Dege	
David Pierce	GE Aviation Systems US
Ed Hahn	ALPA-FEDEX
Ernie Condon	
Frederique Dauvillaire	Thales Group
Hannes Alparslan	
Isidore	
Jerry Hancock	
Joacy Freitas	
John Angemayer	
John Flores	FAA
Judicael Gros-Desirs	AIRBUS SAS
Kai Florian Tschakert	Lufthansa Technik AG
Karan Hofmann	RTCA
Kevin Thomas	
Kornf	
Laurent Leonardon	Collins Aerospace
M. Waheed	Aviage
Mariusz Pyzynski	IATA
Mark J Kelley	AVISTA
Mitch Trope	
Oliver Palumbo	
Philip Watson	Panasonic Avionics Corp.
Philippe Marquis	DASSAULT AVIATION
Philippe Robert	PVM-CS
Ravi Nori	Teledyne Controls LLC
Roman Fischer	Skyguide
Sam Masri	Honeywell International
Stefan Schwindt	GE Aviation Systems UK
Ted Kalthof	
Ted Patmore	Delta Airlines
Varun Khanna	Federal Aviation Administration
Vic Patel	

Stefan noted that we we need further review of ED201. Two additional weeks will be provided for comments. People outside the aircraft base can also participate.

Discussion about possibly providing guidance on how to interact with military started. Hannes Alparslan, mentioned that there is a diff between military in EU vs US. It might be useful to include guidance for dual use equipment. It was noted that military in EU is independent in each country. Each state is separate. There may be more conversion when it comes to ground systems.
It is very nationally dependent. Some already call up the DO-series for airworthiness.
from Hannes A. recommended that we should avoid is to create unnecessary higher implementation costs for civil aviation through the consideration of military “requirements”

Clive asked for a volunteer to elaborate the military area and supply the text.

Stefan provided a reminder for everyone to provide feedback in the next two weeks.

The document is planned to be published in October this year.
Open consult for ED-201 starts tomorrow.
Clive asked for comments from non-authors of 201A, as most comments to date have been from people who have generated the material