EUR 277-17 / WG72-104
RTCA 258-17/SC216-076

St Denis and Washington, 31 October 2017

Summary of the Meeting of RTCA Special Committee 216 (Meeting 35)
EUROCAE Working Group 72 (Meeting 47)
Aeronautical Systems Security

DATE: Sep 12th to 14th, 2017

PLACE: APSYS Airbus Toulouse
RTCA Washington, DC

CONTACT: Karan Hofmann (khofmann@rtca.org; 202-330-0680)
Anna von Groote (anna.vongroote@eurocae.net; +33 1 40 92 79 26)

ATTENDEES:

Name	First Name	Company	SC-216	WG-72	12	13	14
Allen	Severn	Boeing	X			T	
Angermayer	John	Mitre	X				Tpm
Call	Martin	Boeing	X		M	M	M
Castro	Claudio	Embraer		X		Tpm	
Cypien	Cedric	Airbus		X	M	M	M
Flores	John	FAA	X		T	T	
Fuilla	Patricia	Apsys for Airbus		X	M	M	M
Gauthé	Armelle	Apsys for Airbus		X	M	M	M
Gobbo	Giles	Airbus		X	M	M	M
Goodchild	Clive	BAE Systems		X	Tpm	Tpm	Tpm
Grant	Chris	UTC	X		T	T	
Hannert	Larry	LCH	X		M	M	M
Hendricks	Shantinique	Boeing	X			T	
Hennig	Jens	Gamma	X		M	M	M
Hofmann	Karan	RTCA	X		M	M	M
Hrubesz	Marek	Department of National Defence of Canada	X		T	T	T
Jing	Owen	Department of National Defence of Canada	X		T	T	Tpm
Johnson	Dan	Honeywell	X		M	M	M

Kelley	Mark	Esterline AVISTA	X		M	M	M
Khanna	Varun	FAA	X		M	M	M
Leonardon	Larent	RCF		X	M	M	M
Lirong	Tian	Avic	X		Tam	Tam	
Marchand	Cyril	Thales		X	M	M	M
Marquis	Philippe	Dassault		X	M	M	M
Messerschmidt	Michel	Airbus		X	M	M	M
Morrissey	Patrick	Rockwell Collins	X		M	M	M
Nori	Ravi	Teledyne Controls	X		M	M	M
Nyikos	Siobvan Megan	Boeing Commercial Airplanes	X		M	M	M
Pierce	Dave	GE	X		M	M	M
Robert	Philippe	AKKA-Aeroconseil		X	M	M	M
Rosay	Cyrille	EASA		X	M	M	M
Royalty	Chuck	Aerospace Systems Cyber Security	X		T	T	
Safarian	Shohreh	FAA	X			Tpm	
Sampigethaya	Krishna	UTC	X		M	M	M
Schwindt	Stefan	GE		X	M	M	M
Shuang	Zhang	Avic	X		T	T	Tpm
Skaves	Peter	FAA	X		M	M	M
Trope	Mitchell	Garmin	X		M	M	M
Waheed	Mohamed	Aviage Systems	X		T	T	
Waller	Adrian	Thales		X	T	T	T
Watson	Philip	Panasonic Avionics Corporation	X		M	M	M

M meeting, T telephone

1 Tuesday, September 12, 2017 Day One

10h15 Start of the meeting
WG-72 only

No detailed agenda
Objective is to agree on the draft
Go through the Non-Concur (NC) and High comments in priority
Review of the new WP on Risk Assessment (RA) (Boeing, DJ Likelihood example, Ravi Nori and Airbus examples)

1 – Review of NC comments

- Comment #49 NC from Dassault.

From Dassault point of view, corresponding table between SAL and EAL is missing.
Dassault propose to add a new section related to reuse of products already certified according to common criteria
Table from Dan is discussed => comparison between DAL and EAL.
Very difficult to compare and to have a mapping between SAL and EAL
For instance:

- P. Robert mentions that source code review is an objective of SAL3 objective, but not of EAL3 evaluation criteria (Source code review appears at EAL4 criteria)
  - Relevant/good approach to have this correspondence DAL/EAL but need to have it at the correct level.

As summary two topics:
How to apply CC => at item level only
Corresponding mapping could be added but needs to perform the analysis

Seems to be difficult to include a one to one correspondence table between SAL and EAL.
Anyway, traceability tables with CC in appendix D need to be reviewed and improved with a CC specialist

EASA: what is possible for the applicant to demonstrate the compliance is to propose an equivalence that could be negotiated with AA

MM proposes:
To update §4 introduction to explain the reuse of CC evidences + removal of the note
No update is performed in §2.3
§4 is updated in session => OK for the wording. **Comment is closed**

- Comment #280 NC from GE Aviation ED203A vs ED204

Discrepancies between the two documents => misleading/confusing for DAH

§2.5.3 related to Continued Airworthiness: not consistent with scope of the current draft and others statements in the doc

2 options proposed by Stefan Schwindt:
Option 1: Remove it from ED203A and update of a future ED204A accordingly => risk to lose some information because ED204 update not yet agreed
Option 2: Update scope and other sections of ED203A to explain the entire life cycle from DAH is covered => risk of redundant information + significant workload

History:
ARAC report => No change in ED204 and add what is missing in ED203A.

EASA position (Cyril Rosay + JP Moreau on phone):

- ⇨ Preference for option 2.
- ⇨ DAH guidance and related objectives from ED204 will need to be added in ED203A (§8.3 from ED204 to be included in ED203A)
- ⇨ Be careful how it will be introduced in ED203A, will it need some additional text?

Option 3 from MM:

- ⇨ Full DAH guidance after TC in a new document.
- ⇨ Ok but what about the current guidance?

Option 4: to keep inconsistencies as is and explain in introduction the discrepancies.

SC-216 discussions before joint discussions

Varun read federal registrar statement
Discussed how we SC-216 feel about the document
Dan – contradictions in document, might have to do with several methods in appendices
Varun - In Hamburg, had zero success using ED-203 method, would make it a non-concur if forced to use
Siobvan – agree, ED-203 openly referred to as Airbus method, DO-356 openly referred to as Honeywell method, doesn't sit well, that is why as an OEM we (Boeing) needed a Boeing proposed method
Varun – doesn't like the way the document is written
Dan - Too much detail, not mature

Joint WG-72/SC-216 session

Dave – seems unlikely to several people here that doc is ready, need to figure out plan
Michel – concerns should be submitted as comments so we can address accordingly
Dan – concerns are broader than text
Discussed Dassault non-concur comments
Philippe is in the meetings but needs to socialize responses and discussions with his company
Michel – move onto discussing new non-concurs

Non-concur comment discussion

- *First new non-concur discusses Continued Airworthiness (ICA) and how it should be addressed in this doc and DO-355/ED-204* - NC comment #325 from Thales:

About SAL allocation regarding security measures that are not security functions.
For instance, interfaces or source code hardening in legacy programs currently not taken into account whereas could be seen as a security measure as this is a kind of protection
Are source code hardening rules can be considered as an assurance activity? Dan thinks so

Clarification of what can be considered as a security measure => Michel proposes to update §3.5. Security measure does not necessary means security function. A security measure does not need to add functionality

Dan – already removed detail from 2.5, removing more will make it worse, personally I think we need to go to working paper contents to get useful info for ICA
Varun – are you (Boeing) OK with DO-355?
Martin – yes

Dan - Operator side good, what about developer side?
Vulnerability and threat management part of 2.5 is probably the most controversial part
Dan will submit a comment regarding this tonight, don't need to discuss here as we have other things to cover

⇨ **Comment still open, Dan will make a proposal**

- *Next new non-concur in 4.1.1, SAL2 objectives seem to be applicable to security function only, would like to be able to address reinforced robustness of interfaces in legacy SW…*

Cyrille M. from Thales explaining comment/concern
Martin – Security Assurance Levels (SAL) need to be re-examined, what is required for each, look at it from hazard level
It says SAL 1 doesn't count for anything
Dan – you have to do risk assessment to see if you have SAL 2 or 3 situation
Martin – do risk assessment no matter what
Varun – I think you are saying the same thing
Martin – SAL 1 for minor or no effect conditions, amount of work you have to do to prove security measures are robust enough, right now as written, seems SAL 1 is useless, need to be able to use it otherwise it won't make sense
Siobvan – we try to give meaning to SAL1 in the Boeing proposed method in the appendix, in one of the checklists
Martin – need to take credit in situations where the minor or no effect system is the interface to something else
Phil – committee focused on security as it pertains to safety
Martin and Varun discussing propagation
SECSE -> Security Event that Causes a Safety Event
Peter - DO-178 is a process doc, not requirements doc, intended function, security is outside those documents, the requirements are what is weak
Ravi - What about appendix tables for SAL1?
Hardening source code as security measure?
Dan – hardening is part of assurance activities (SAL 2 and 3), measure itself is OS that we need to harden
Martin – grey area on hardening and what can be used toward security credit
Martin to submit comment on rephrasing bullet on SAL 2

- *Last new non-concur comment on security logging*

About event logging:
Currently we have some requirements in §4 on how we manage security incidents
But the question is how do we deal with §6.2? There is no link between section 4 and section 6 dealing with logging. No corresponding objectives in §4? Is it really needed?
Security logging can be seen as a kind of security control or mechanism (prevention) but can also be used for forensic.
What is the real need?
§6.1 First sentence => it is essential to monitor security measure effectiveness
§4.6.2: Propose to add a new objective O12.x to require the capability to monitor security measure effectiveness => for SAL3 only, applies to AC,S, I) + associated activity

Cyrille - In section 6 there are CONOPS for this
Set of objectives and activities
What do we really intend from section 6?
Should link objectives from section 4 to CONOPS in section 6
Mitch – applicant decision on how much you monitor, depends on security architecture of aircraft,

there are architectures that don't require detailed logging
Logging isn't the only solution to monitoring, requirement to log should be driven by architecture, not this document
If you don't have an input by design
Chuck – logging not required for all functions, compare to FOQA data
Martin – what is the alternative?
EICAS, security events recorded, can look at later
Chuck - Don't want to equate warning system with security logging, not examined on airplane in real time
Pilot not going to be trained in cyber
Look at maintenance record, not EICAS
Dave – logging hasn't resolved anything yet
Varun - DAH is responsible for enforcing what needs to be logged on your airplane
Stefan – time to put together proposal to address this
Dan – alternative is to apply at aircraft level
Chuck – logging not automatically implied
O12.x The capability to monitor security measure effectiveness is established
Chuck - If you can't detect that something is not working, assume it will eventually not be working, need code to ensure it is working properly
Heartbleed example
Martin – cannot design for what you cannot know yet
Went back to whether or not you need specifically logging to meet objective
Peter brought up Built In Test (BIT)
Ravi – example or whether logging is needed, OS that is 20 years old, deal with this at Teledyne, OS not supported, limited storage capability, if you do logging, can only store for a day, might not be able to offload
Is logging going to help here? No for this intended system
Martin – legacy system, don't need to do anything
Something brand new, depends
Stefan – we are arguing about shades of grey, not making progress

- ⇨ **Added objective, Comment is closed**

Dan presented Likelihood Evaluation of Threat Scenarios
Power point instead of working paper
Steps

- Determine security scope
- Determine architecture and measures
- Characterize threat scenarios
- Use likelihood evaluation to evaluate scenarios
- Consolidate…

Numbers and qualitative factors
Exposure reduction contingent on attacker as well as aircraft mode, attacker gets to choose
Clarifying assumptions for this example…
Interface between cabin and maintenance network for this
Responsibility is maintenance network, part of security environment
Not looking at passengers
In this case, must protect yourself
What design features do you want to take security credit for?
Michel – cabin services could be another asset
Dan – systems hosting those services could be an asset
Threat scenarios for this

- Admin password, gateway configuration

- Passenger flood
- Passenger, cabin services flood
- Passenger, gateway IP password gateway, configuration

Walking through each threat scenario…
Martin – a couple ways to evaluate control
Dan's method - Trust security control to DAL of system
Another approach – can use a higher number if you can show with SAL objectives
Dan – I like DAL, but you can use another method to determine that number
Ravi – confirming you don't have to use a graphic threat tree, can use tabular
Martin – prefer cut sets too, easier for reader
Finished going through presentation
Looking at Ravi's example which he emailed to 5 committee members, not on workspace yet
Martin – if you can do two things at the same time that have minor effect, what is the overall effect?
Peter – credit for independence
Plan for tomorrow morning – go over Siobvan's Boeing proposed risk assessment methodology working paper and comments

SC-216 only

Discussion on sticking points of committee and current document
Turn those into comment per Michel's suggestion?
Varun – during Hamburg meeting, an example that took Teledyne 10 min to resolve took 8 hours and even then couldn't resolve with effectiveness method (i.e. ED-203 method)
Ravi – couldn't come to consensus on what problem we are trying to resolve, only one person intimate with method present, Airbus security architect
He couldn't explain how he assigned the numbers/points
Michel has been reaching out to committee members individually to get a feel for how this is going
Ravi – eliminating methods not an option, need to give the applicant a chance, suppliers will hurt the most, OEMs will have more leverage than suppliers, need to give guidance to suppliers
Martin – what is the right level of detail?
Patrick - Don't want to write document that constrains us, new methods emerging, internally can use a different process and have a good product
Costs a lot of money to change process, won't make product better
Peter – regulators don't want multiple processes, having said that don't want it to be so rigid no room for flexibility
Varun – let each applicant decide based on architecture
Catch 22 – need workable example otherwise hard to follow process
Dan - Risk assessment methodology has replaced threat scenario analysis
Peter – 178 and 254 have been around for a while and they still have training courses, how are we planning to train the work force in 356?
Chuck – takes years to become an expert, how do you train a safety aerospace person into a security person?

Can you take credit for COTS security function?
Impact and extent of failure?
Martin – security controls now may not be sufficient 40 years from now
Patrick – true for crypto, in other spaces there could be new vulnerability in a part
Ethernet switch – cheap COTS component, widely known, good if configured properly
Don't spend too much time on strength of characterization
Varun - Binary – controls either work or they don't

Siobvan – sanity check – is the main difference between the methods in how to determine likelihood, i.e. effectiveness, ease-of-execution, etc.?

Dan – I thought so but examples have shown otherwise
Larry – WG-72 - Risk assessment on threat scenario basis
Dan – I don't see them doing it

Patrick – reader needs to get educated
Ravi – who trains you? And using what method?

Peter - What is the risk if we keep using issue papers, use docs as guidance, but let industry come up with their own solutions? Boeing could have their own standard that they flow down to suppliers
If documents aren't mature enough when published, don't want to require them to be used
Want to publish but also want to make sure major companies are willing to use them
Dave – 326A for sure has been used, not 356 yet
Varun – young documents, will be revisions, but shouldn't happen immediately, revise as things progress and we see usage
Discussed evolution of DO-178

Martin – want something both FAA and EASA agree with
Jens – is there consensus between the two regulators? If not, how do we go about that?
Varun – I prefer simple, Europe is the driver of this detail

Dave is taking notes on issues we take with ED-203 method, can discuss during joint method tomorrow

Want to get back to Martin's concern on SAL 1, how we currently don't care about it but it should have more meaning
Martin – Don't want to say we don't care about minor and no effect systems, otherwise the suppliers and system owners at our own company won't care about implementing security requirements
Peter – aircraft not connected that much to ATC *electronically*, able to get away with mismatch, as we become more connected it becomes more problematic
No way to evaluate in certification if you implement controls in EFB
Martin - Can do so in part 121

Plan for tomorrow: Siobvan to go through working paper and comments, then we will go through our general comments and concerns for the paper for Michel, then we will discuss if we are ready for FRAC
Ironic that WG-72 is pushing for FRAC and SC-216 is not, usually the opposite
Thursday late morning we will vote as a joint committee if we are ready
Rest of time – comment resolution

Don't need to resolve everything prior to FRAC, but at least non-concur and high comments
Currently addressed all non-concurs
SC-216 non-concur comments not formalized, we need to be more responsive in reviewing entire draft
Larry – recommendations to accompany comments?
Comments list generated mostly by WG-72, manageable
270 pages to harmonized doc so far
By comparison, 356 Rev New is 80 with only 55 pages of real content
Advantages and disadvantages of FRAC?
FRAC forces people to take a stand
46 high and noncompliance in spreadsheet

Looked at schedule again

- December meeting may be moved back to DC since Melbourne was impacted by Hurricane Irma
- If no November meeting, traded for October
- These meetings need to be announced and in the federal registrar to be official plenaries
- Will ask Karan for specifics

SC-216 dropping the ball on reviewing doc in its entirety
Another issue is that it is hard to keep track of what is the current version of the doc that we should be reviewing, can make comments on one section, then it changes and it might change the comments
WG-72, particularly Airbus, making the majority of the comments
Key is giving the document a thorough review, even if it delays FRAC
Karan – can do an "internal FRAC"
2-5 tomorrow – review individually?
Multiple people unhappy with objective tables
Ravi – should probably talk about Michel's uploaded example tomorrow
Dan – problem is text, not example
Send email to Dave if you think of anything that needs to be discussed

Adjourn

2 Wednesday, September 13, 2017 Day Two

10h15 Start of the meeting
WG-72 only

SC216 wants to postpone the open consultation (due to lack of review by SC216, probably due to the length and complexity of the document)
But we will never have 100%.
There is a need to freeze the draft in order to allow the review. Too many versions during the summer.
How do we want to manage track changing?

MM reminds the main objective:
First to complete the remaining parts, then to harmonize the document.
We also need to have external opinion at this time.

Review of documents sent by SC216:
Discussion on how to reduce/simplify the document:
The current draft addresses some complex topics so it is difficult to simplify it
How can we simplify/reduce the complexity of the document?
Harmonization objective is reached => one document!
Maturity on the way to be achieved, it will come later, normal work
Need to have a basis to improve later
We have constraints regarding harmonization and ARAC recommendations => This will not reduce the size of the document

Discussion on SAL:
Definition of SAL should be improved. They are not anymore in line with their foreseen purpose.

Discussion on ED204 vs ED203A
What can we propose to SC216?
ED203A should be an AMC.
We need to define the final target. What should be in ED203A and what in ED204?
Content of §2.5.1 has been replaced by ref. to D204
From SC216 point of view, means this § section no longer s complies with ARAC recommendations ad WP 2.5 => suggest to restore §2.5
Still some discussions on discrepancies between ED204 and ED203A

Joint WG-72/SC-216 session

Reviewed summary of SC-216 comments with WG-72 - E-mail from Dave:

- ⇨ Complexity of the document as it was not sufficiently reviewed.
- ⇨ WG72 discussion this morning:
  - o surprise as decision should already have been taken during July meeting, few comments received until this week
  - o in 6 weeks we'll still meet the same issue, so we need to pinpoint the part to be improved
- ⇨ Proposal is to use the December meeting to vote for FRAC/OC but need to align on what to be done in the meantime
- ⇨ A lot of high comments to tackle with => another argument to delay
- ⇨ Commitment from SC216 to provide all comments for the 13rd of October. Only detailed comments with proposed answer will be acceptable.
- ⇨ November meeting should be kept to discuss comments resolution and FRAC/OC in December

New comments from Dan on behalf of Honeywell to include non-concurs
Varun – don't want to keep reviewing it piecemeal, need to review as a whole, difficult due to summer breaks and other work assignments
Huge amount of input from Europe over past 6 months, lack of review from SC-216, will be a hard deadline at next decision point, time is required to review doc in total, next review will be full and final from SC-216 perspective, and if people don't comment we will proceed regardless
Close but there still needs end-to-end review
Stefan – agree, that was the point of this meeting, supposed to do FRAC decision in May
Dan – in May, it wasn't a complete document, shouldn't count, only one delay
Disagreement between committees on how many "delays" there have been, has to do with how many drafts there have been and disagreement on extent of changes

Current status – SC-216 does not think this is document is ready for FRAC
Michel says no indication before
Dan disagrees and has voiced this before
Stefan – if you didn't review it due to other work commitments, tough, need to proceed
Varun – fair enough
Stefan – need new date in federal registrar for Open Comment (OC) meeting
Dave – use December meeting as new meeting for vote for FRAC
Varun – that will be the last meeting where we vote
Michel – what needs to be done to document on this time
Dan – 42 comments on first 3 sections sent, includes 7 additional non-concurs
Dave – we were planning to review the document in the afternoon, use that dedicated time
Varun – priority to review non-concurs up front
Karan needs two months after document is done to get publishing aspects sorted out
If we are done with document in March, will be May or summer before published
FRAC and OC is not an opportunity for the committee to keep working the document, it is specifically for the public to comment

Decision – publication of document and corresponding schedule will slide right
Deadline for SC-216 to finish reviewing document in its entirety – October 13
Dave - November meeting might be OBE, but we could use it to disposition comments
Dan – might still need to meet face-to-face to disposition comments
Michel will not be available most of October

Looking at architecture example again along with Michel's new example posted yesterday
Discussion/arguing over example
Airbus example on RA

- Discussion about the threat scenario that should be described in a more formal way and should contain more information
- Preliminary RA done at design level in several iterations with different assumptions => can be considered as the RA iterations from ED203A
- First identification of Initial risk, then risk treatment for risk mitigation =>aim is to achieve the risk acceptable.
- Example is not realistic but it can demonstrate that the method is able to discover a big mistake
- Main difficulty is to determine the effect of the SM. At first it is an evaluation to induce the determination of the necessary SM. At the end, there is a need to verify through verification and refutation that the effect is consistent (substantiation). At the beginning, scoring is a way to evaluate and compare the different options in order to identify the best one.
- How does the risk evaluated go back to safety assessment? Safety will reassess the risk based on the new architecture that includes security.

- Example shows all iterations that bring to the final PSSRA that is provided for certification and only contains the chosen option.
- RA provides the objectives and then are translated into requirements for the development of SM.

Chuck – I don't know how to approach this as the example seems unrealistic
Reminiscent of an IT system, not embedded system
Need more detail before working
If a security person brought this to a systems person, they wouldn't know what to do with it
Patrick – more detailed example from avionics?
Martin – we could, but I don't think a more detailed example will help, will still pick at the same things
Martin's general concern – end of method where you put the evaluation, how do you decide on value, did you do enough, is it sufficient to protect aircraft
What if you have enough points but there are still holes? This is where security engineering judgment needs to come in
Michel - All methods have possibility of overlooking something
Martin – agree, but would like to see tie into right type of testing to support analysis, not requirements testing, talking about robustness, security, penetration testing
Can someone other than analyst find holes in it before airplane goes into service?

Chuck – sounds like different purpose, robustness part of development, purpose of this is to provide certification evidence
Guide verification activity rather than provide cert evidence?
Stefan – don't have guidance for that type of testing, that's why we are looking for a volunteer to provide an example for what that testing will look like
Patrick - Statement that inclusion of optional security measures and architecture not part of cert package are for information only
Phil - Security hopefully has influence on aircraft design

Michel – propose to add this paper to appendix E
Martin – great example, but it's too much, if you put this in the appendix, even if you say just an example, you will get people who find compliance to direct you to this paper for cert evidence
You don't need to supply requirements as part of cert evidence
Chuck – tension between two groups, when looking at length compared to other standards, others don't identify engineer interactions
If not outcome, go back and fix it
Valid point that if you include this method example, it is liable to be perceived as the method, maybe rename it to be clearer?
Take break, then discuss text to go into document, what will actually be included

Draft of what we want reviewed before we all leave tomorrow
Dave reminded everyone that Siobvan was supposed to present Boeing proposed methodology and how comments were addressed so far
Siobvan – Either we have no methods in the appendices or we include the Boeing proposed method, especially since there is an Airbus method and Honeywell method
Michel doesn't have a problem with this, already incorporated working paper Rev A text as an appendix, wants to use this time to concentrate on non-concurs

Took a vote in SC-216 room, 100% agree document is too complex
Varun – want to take next 3 weeks to review before giving the definitive answer on level of complication
Michel – do nothing during 3 weeks?
Varun – no, can work current comments while waiting for new comments

Michel going through non-concurs in comments spreadsheet

Review of the comments:

- Complexity of the document
    - Should be addressed with the detailed comments that will arrive.
    - Distinguish considerations and guidance in all chapters could help.
    - Review of chapters: 2 OK, 3 is in the way to be OK, 4 OK no way to simplify, 5 seems OK rather short: provides the main principles for architecture, 6 is short => 107 pages
    - Review of Appendices: 157 pages contains details, examples of methods => need to agree on the content, it was the initial request to add examples and now, it is challenged…
    - Need to improve the introduction in order to help understanding

- Comment #118: NC from Boeing => Closed

Siobvan confirmed that the non-concur comment from Hamburg is closed with edits to 3.6 plus new appendix added

- Comment #341: NC from DJ
    - ED203A vs ED204
    - Both options 1 and 2 seem acceptable but there are different implications. Option 2 requires more workload
    - SC216 in favor of option 2. Solution remains to be decided
    - Dan will provide the last agreed paper that needs to be integrated in chapter 2
    - Dave will make a proposal
    - Details below…

Updating DO-355/ED-204
Would be a major update
Right now, make sure we are in agreement with the current 355
Dan - Current ACs only invoke 355 for operators
Michel - ED-204 also invoked in SCs
Question to John Flores
John – 355 still has info for DAH as well, though primary is for operators, DAH need to provide ICA info to operators in compliance for SCs
Varun – last bullet of SCs covers procedures
Dan addressed that things have mysteriously changed (makes difficult for review)
2.5 working paper proposed text worked well to address
Disagreement between Dan and Michel on what should go into 2.5
Dan - 203A already talks about need to supply security guidance
2.5.1 talks about security guidance contents

Stefan and Dan discussing options for where to handle ICA
Important since this was part of ARAC report recommendations
Varun – should be a section re: From Ops point of view, these are the DAH responsibilities and these are the Ops responsibilities
Dave - Bring DAH from 355 to this doc – all or just related to developing guidance? Wondering if Ops is included
Stefan – still open, operations side still missing vulnerability management
Option 2 – update scope and any other place so it states ED-203A will cover the entire aircraft life cycle from DAH…
More like modification – proceed with option 2 but not complete option 2
Dave volunteered to help with this one

WG-72 needs to leave soon, still 5 or 6 non-concur comments they want to go through tomorrow
This afternoon, SC-216 will do their individual review
Boeing proposed methodology bumped to tomorrow morning, no changes from Rev A on sites

SC-216 only

"Study Hall" – everyone reviews ED-203A/DO-356A individually, ask questions as needed, and develop comments

Adjourn

3 Thursday, September 14, 2017 Day Three

10h15 start of the meeting
WG-72 only

Clive's proposal regarding the management of comments is discussed. Proposal is agreed except for the scope. Michel proposes to affect 2 persons per topic and not per chapter.
All comments are classified by topic (level of threat, security assurance, ...) and we propose to assign all comments on the same topic to one editorial group.

Each editorial group should at least consist of 2 persons and members of SC-216 and WG-72. Every WG participant should contribute in the editorial groups to avoid that few persons tackle most of the comments (concern of further delay due to workload).

Comment resolution rules:

- A proposal should be made by the author of the comment. If not the comment will be rejected
- For comments on figures, the author of the comment should propose the updated figure and include them in the "Attachments" worksheet of the comments file.
- A rationale is required for classification of comments in NC and High categories. The classification of comments has to be done according to the rules in the "Help" worksheet of the comment list.
- At least 2 persons per topic: one for SC216, one for WG72. Each person should have less than 5 topics. At least one topic per person.
- Comments resolution from the editorial groups should be included in the "Resolution proposal by subgroup/editor" field.
- History should be kept in column "Resolution proposal by subgroup/editor" with the identification of the editor and date
- Comments resolution updates from the editorial groups will be sent to Michel who will maintain the "official" list and distribute updates through the workspace
- Comments shall be handled in order of priority, first focus on NC and High comments
- Existing NC comments will be handled by the whole WGs **from now on**
- WG-internal reviews should be completed and comments submitted to Michel **until 13. Oct 2017**
- Editorial groups provide resolution proposal for all "NC" and "H" comments until **3. Nov 2017**, "M" comments as far as possible

Affection of WG72 people for each topic of the list is done. This will be presented this afternoon to SC216 and SC216 will be asked to do the same this afternoon.

Schedule
Target date for WG internal reviews and comments: 13th of October
Resolution proposal for all NC and H comments until 3rd of November

Weekly telecon: should be maintained for the review of NC comments per topics. Schedule to be defined by SS and fine-tuned regarding needs and availability of people.

Review of NC comments

- #344: comment rejected as in contradiction with ARAC recommendations and already discussed during Phoenix meeting in February 2017

Linked to comment #398: OK, first bullet should be part of the normal text

- #371: Need to justify why it is a NC + Dan to propose an alternative to the list

Joint WG-72/SC-216 session

Schedule discussion – WG-72 proposal as follows (from email)

Agreement of the 2 groups that we don't go for FRAC/OC this week ant that it will be done during December meeting

Discussed Clive's proposal in the joint session (see previous page for proposal and comment resolution rules)

Editorial groups divide up work
However, coordination needed between certain sections
WG-72: Comments should be accompanied by solutions, otherwise they are rejected
SC-216: Certain cases where we can't get the solution in time by October 13, for example, editing figures, shouldn't be an automatic rejection
WG-72: Non-concur and high comments need to be justified
SC-216: Can't reject these comments, otherwise you'll get a dissenting opinion or non-approval of the document
Karan – if you have a non-concur at FRAC and don't address it, that company can put in a dissenting opinion, messier to handle it that way, whoever puts in the non-concur needs justification or alternation, and group as a whole needs to decide how to address
Long story short, can't simply reject a non-concur, everyone's voice is heard
Dan doesn't want justification per this table, OK as advisory but not mandatory
Dave – doc needs to be technically accurate and applicable to our industry
Varun – good list, but there might be good justifications out of this list; that was Dan's problem
Martin – no need to argue on this, SC-216 is not going to let a comment slide

Stefan – the plan we already have will extend this an additional 3 months
Reviewing proposed updated schedule
Karan - Backup plan if we don't get an agenda released in time to make it an official plenary – PMC agenda for December already submitted, release of FRAC documents is a topic, on December 19 someone from SC-216 can appear or call in
Karan needs document first part of May to get this released during summer when FAA needs this
New schedule possible, assuming we don't get an excessive number of non-concurs

Going back to how to handle comments
Categorizing comments by topic – some can span several topics
WG-72 People assigned to editorial leadership in different areas, SC-216 can be assigned as well
Dan – don't need independence between editor and commenter
SC-216 members volunteering for different topics
See spreadsheet for complete list of assignments

To summarize…

- Concern on the update of figure
- Reminder on the definition of NC and the need to provide a justification agreed by Karan
- FAA has the agreement for a 3 months delay. SC216 commits to provide comments on time. FAA asks people to keep focus for issuing the document despite the lack of time people could encounter and really resolve all comments
- Presentation of the list of topic and editor group
- For NC comments the resolution will be agreed by the whole working group
- Multi topic comments will be discussed with concerned editorial groups

Schedule

- October 13th: draft review completed and comments provided
- October 23th – November 3: Comments resolution in editorial groups
- November 13 – 17: Comments disposition Meeting
- **December 11 – 15: FRAC / OC disposition**
    - That means official launch should be beginning of January 2018
    - 45 days duration for open consultation
    - Comments resolution moved to April 2018
    - New meeting early May Final disposition meeting for publication before summer (deadline for RTCA/EUROCAE approval by summer 2018)

Please note that the publication will depend on the amount of comments we will receive.

Siobvan and Martin presented Boeing proposed Cybersecurity Risk Assessment Methodology (CRAM)

Notes/comments/concerns:

- Make assets and security requirements both inputs to step 1 system/airplane characterization (Patrick)
- Lots of discussion on ease-of-execution and why it should be a consideration, pointed to other places in the document that deal with it
- Make sure HMU is in example architecture, Phil couldn't find it in draft harmonized document
- Need to be more specific in operator guidance and what drives a change
- People were picking at the example itself and USB and lost focus on the process
- Chuck is concerned that ease-of-execution should stand on its own and it might say the risk is lower, Boeing is arguing that it actually adds rigor and says the risk is higher / takes a more conservative approach
- Not analysis along, testing involved as well
- Will use a better example with more analysis and watch the comments roll in

WG-72 session ended, SC-216 only in afternoon
Varun – SC-216 cannot drop the ball again, we have to review prior to October 13
Propose different people start reading at different points as up front material gets reviewed more thoroughly than following sections

Meeting minutes from last time not posted yet, **still waiting on EUROCAE number**

SC-216 only

Study hall

Adjourn

4 Main decisions and actions

Decisions		
Postpone FRAC until December		

Actions	Who	When
Review document and provide comments and suggested text and diagrams	All	October 13th

/s/
Siobvan Nyikos
Secretary, SC-216

/s/
Clive Goodchild
Secretary, WG-72

CERTIFIED as a true and accurate summary of the meeting