RTCA Paper No. 003-17/SC216-065
January 3, 2017

Summary of the Thirtieth Meeting
Special Committee 216
Aeronautical Systems Security

DATE: December 12-15, 2016

PLACE: The Washington Campus (same building as RTCA, Inc.)
1150 18th Street, NW, Suite 400
Washington, DC 20036

The Committee wishes to thank The Washington Campus for hosting this meeting.

CONTACT: Karan Hofmann, RTCA Program Director
Email: khofmann@rtca.org

ATTENDEES:

SC-216 Co-Chair

David Pierce	GE Aviation

SC-216 Secretary

Siobvan Nyikos	Boeing Commercial Airplanes

Designated Federal Official:

Varun Khanna	Federal Aviation Administration (FAA)

Members attended:

Karl Frantz	GoGo
Raoufou Ganiou	TCCA
Chris Grant	UTC
Larry Hannert	LCH Engineering
Karan Hofmann	RTCA, Inc
Mark Kelley	Esterline
Bernie Newman	Astronautics Corp of America
David Robinson	FAA
Shohreh Safaria	FAA
Mitchell Trope	Garmin
Mohammad Waheed	Aviage Systems
Phil Watson	Panasonic

Members attended by phone:

WG-72	EUROCAE
John Angermayer	MITRE
Raphael Blaize	Airbus
John Flores	FAA
Christian Fiore	MITRE
Owen Jing	Department of National Defence of Canada
Michel Messerschmidt	Airbus
Dinkar Mokadam	AFA-CWA
Cyrille Rosay	EASA
Chuck Royalty	Aerospace Systems Cyber Security
Romuald Salgues	Airbus
Stefan Schmidt	GE
Tim Tinney	Saab Group

Note: Attendance was recorded via the verbal roll-call, the sign-in sheets at the meeting, and the list of people logged into the WebEx. Apologies if anyone was missed.

In accordance with the Federal Advisory Committee Act, Varun Khanna, Federal Aviation Administration (FAA), was the Designated Federal Official.

This meeting consisted of both plenary and working sessions.

The outline for this meeting summary is organized around the published agenda. SC-216 presentations and documents can be found at the committee's Workspace site at http://workspace.rtca.org . Please contact the Program Director for access to the site.

Details of document edits are generally incorporated by reference in this summary. The agenda was published in advance of the meeting, and is available from the RTCA website.

Meeting Summary

Day 1

Varun Khanna: Public meeting announcement:
In accordance with the Federal Advisory Committee Act, this Advisory Committee meeting is open to the public. Notice of the meeting was published in the Federal Register on November 18, 2016. With the approval of the Chairs, members of the public may present oral or written statements. Persons wishing to present or obtain information should coordinate with the RTCA Program Director Karan Hofmann and Chairs David Pierce and Daniel Johnson.

Karan Hofmann: RTCA proprietary references policy:
RTCA seeks to develop standards that don't require proprietary information for compliance. However, patented technology and copyrighted material that are required for compliance may be included in a standard if RTCA determines it provides significant benefit. If your company holds a

patent or copyright relevant to an SC-216 document being developed, advise Karan Hofmann, Dan Johnson and Dave Pierce.

Karan Hofmann: RTCA membership policy:
Organizations with a representative participating on RTCA Committees must be members of RTCA.

The Chair Dave Pierce opened the meeting and introductions were made around the room. The agenda was reviewed, and the minutes of the last meeting were accepted.

Began with Joint SC-216 & WG-72 meeting

WG-72 presented ARAC ASISP report: impact on ED-20x development (Cyrille Rosay, EASA)

- Published by FAA November 30
- How to read? Jump to list of recommendations, one closest to WG-72 and SC-216 objective is "adopt existing standards…"
- Or filter recommendations by allocation, i.e. assigned to SC-216 and / or WG-72
- Recommendations 03, 05, 07, and 08

Showed specific GM o be addressed, GM = Guidance Materials

- GM8 scope of security ICA, duplicate of recommendation #7
- GM9 event logging and compliance with 14 CFR 21.3, duplicate of recommendation #22

Recommendation 11 – how to deal with rotorcraft? They would like to modify our standard for their use, tabled until next meeting to allow time for SC-216 and WG-72 to get input from rotorcraft community

- Subgroup of rotorcraft, what is the expectation?
- Alternative, develop AC tailoring ED-20x to rotorcraft
- Stefan Schmidt- We got Boeing name, Eric Lieberman, but Boeing is mostly military so not sure of input, waiting on Sikorsky (bought by Lockheed Martin), also need to talk to Robinson
- Dave Pierce – Serge Barbagelata from Airbus Helicopter, didn't seem to think we needed to tailor much, but could still use standards
- Stefan Schmidt- Logging might not be applicable to helicopters
- Varun Khanna – logging must have a purpose/benefit

Conclusion

- GM1 to GM10 (5, 7, 8, 9, 22)
- Harmonize with SC-216 (5)
- Make something special for rotorcraft
- Add guidance for logging

Scope of SC-216

- Stefan Schmidt– how much flexibility does SC-216 have? There are chapters in the TOC that don't fall into the categories of the ARAC GM and recommendations
- Dave Pierce – we would interpret ARAC material as tightly as we can because there is a lot to do by December 2017, take lessons learned to continue other work later
- Michel Messerschmidt – useful to look at all objectives now and make a plan that goes beyond next year

- Dave Pierce – we need to publish most necessary pieces by end of next year and then handle outstanding issues later

Prioritizing work

- Stefan Schmidt- Can we make similar risk assessments for same product? Higher priority than logging
- Varun Khanna – for rotorcraft, shorter window of exposure and duration of flight, though we were clear on where it is headed, but still need them here to represent their interests
- Bernie Newman – Airbus helicopter may think different
- Varun Khanna – logging more important because it affects part 25 directly

After presentation, looked at the report itself for further detail

- Risk acceptability, looked at tables 2.2-2 and -3 examples
- Chuck Royalty – when we look at these tables, it leaves out important architecture info, assurance doesn't necessarily mean we are going to get the reliability rate listed
- Bernie Newman - Likelihood of threat vs. effectiveness of security measure, during ARAC meetings they said either method would be acceptable
- Stefan Schmidt- How do you objectively produce a risk assessment with the table?
- Dave Pierce – we are OK with adding guidance to make the table(s) usable
- Varun Khanna – use engineering judgment
- Michel Messerschmidt – describe where we use it and where we don't, need to get to same or similar result
- Dave Pierce – work to make it repeatable
- WG-72 - By end of January, both groups finish active work on risk acceptability matrices / tables and exchange, discuss during February meeting, is this possible?
- Larry Hannert – want to focus on TOC sometime this week
- Dave Pierce – falls into working paper for chapter 4, would like to resolve sooner than later

Trust discussion

- Concern that different people can't agree on what is trusted vs. not, and to what degree
- Could go airport by airport and country by country and get different answers

Looking at recommendation 7, does DO-355 need to be reopened?

- During ARAC discussions, Romuald Salgues said it could be handled via DO-356
- TOR says we are only opening DO-356, it is in best interest of SC-216 to limit to scope
- See what changes are proposed, titles, etc.
- To get through type design, there might be additional guidance for DAH
- Varun Khanna – if we have to open DO-355, we should wait until we achieve the goals for this year, opening DO-355 is a longer term item
- Guidance more appropriate in DO-355 or 356?
- WG-72 showed Airbus presentation on missing or incomplete ICA
- Requesting to reopen ED-204 and DO-355, consider connection and consistency with FAA AC 119-ANSP
- Alternative – import considerations into ED-203 and DO-356 and limit scope of ED-204 and DO-355 to guidelines for operators

Major/Minor discussion, what US does vs. what Europe does is different

- Chuck Royalty explained M/M process and if a change is major, we have a cert plan and submit compliance data, need to do all that is necessary for certification unless previous compliance data applies
- Europe – Their DER is not allowed to approve a Major change
- US – DAE or AR can determine a change as Major
- Varun Khanna – still need to do Change Impact Analysis (CIA), security is protection mechanism, not primary function of the box
- Is the issue criteria for MM? Is it the impact analysis for security? Is the impact analysis for systems good to be applied to security?
- A couple issues, one – WG-72 says there should be a separate MM classification for security so that you don't have to use safety
- Two – want to make sure we (US and Europe) consistent in what we consider major
- Siobvan Nyikos – we are not that different, we have a D6 document we use for MM determinations with a separate section for major criteria for network security, will "sanitize" that criteria so that there is no proprietary info and provide for information, make sure we are consistent
- Looked at 8110.49 software section
- Siobvan Nyikos will post sanitized criteria and support a working paper on the topic if needed

End joint meeting, begin SC-216 plenary

Siobvan Nyikos showed sanitized criteria

- Consensus is to include as example material in an appendix with the statement that all applicants have their own tools and processes for MM criteria, but here are some considerations
- Write short working paper and proposed text for appendix with more generalized criteria

Larry Hannert asked Varun Khanna about rules for use of ARAC report text
Karan Hofmann – it's public domain, as long as there isn't a copyright, it should be fine. This has been confirmed with the Office of Rulemaking; specifically, it is important to note and important to not misguide the reader that the ASISP recommendation report contains recommendations to the FAA and it is not the FAA's final position on the issue. If we include a statement along that nature in the RTCA document, it should be ok.

Looked at definition for unauthorized electronic interaction (IUEI)

- Varun Khanna – take advantage of physical barrier as protection
- EMP out of scope
- Electrical – does it mean power or data?
- In answering assessment questions, if it is power only, not applicable

Discussion – if someone has to do an STC and requires OEM data, how do they proceeds? Need input from Panasonic

- Someone has to pay to get data, cost gets passed to customer
- Design architecture so you don't touch the rest of the architecture? Difficult
- Burden to STC applicant

Looked at GM 3, 4, and 5 which ties into risk acceptability tables/matrices, needs text that supports use of tables in 2.2

- Action – SC-216 suggests ARAC 2.2.4.1 forms basis of DO-356 section 2.1
- Action – SC-216 suggests ARAC 2.2.4.2 forms basis of DO-356 section 2.3
- GM 6 and 1 – include text from ARAC, rewrite for clarification
- "Reductions in the qualitative event likelihood should be conservative and based on factors that are under control or can be verified"
- Environment, assumptions, etc. can change over time

DAL E discussion

- Varun Khanna – not concerned with DAL E unless you try to take credit for security controls at DAL E
- Chuck Royalty – all it means is no safety level impact if it fails
- Varun Khanna's concerns with level E (or IFE) systems: It doesn't catch fire and it doesn't interfere with other systems
- System owners of DAL E systems do not want security driving the DAL level and that will increase the DAL level and thus increase costs

Day 2

Began with Joint SC-216 & WG-72 meeting

Went over items we are ready to discuss with WG-72

Ready to discuss IUEI = Intentional Unauthorized Electronic Interaction

SC-216 is hesitant to address rotorcraft until we get DO-356 done since it is not part of the TOR and the rotorcraft community hasn't been attending the meetings

Logging data discussion

- Varun Khanna – not a single action has resulting in log data collection in the 6 years that logging has been required, it needs to be value added, need to do something with it, define what we intend to get out of the data
- Problem for OEM – collect data and have tools to process, but airlines don't
- Data comes without context, i.e. who had access, info on environment
- Sounds great in theory, but we're aren't doing anything, so more about perception
- Will go through logging paper, see what positions are, and take it from there
- Michel Messerschmidt – needs to be process for how we deal with logging data
- Dave Pierce – we will discuss logging this afternoon so we are ready to discuss in joint meeting tomorrow morning

Minor and lower assets

- Varun Khanna & Phil Watson - Minor and lower assets can still be protected, it is from a business standpoint, not safety
- Going back to logging, owners of IFE systems can use logging for business purposes
- From this perspective, belongs in different document, not in scope of DO-356
- Phil Watson - If a minor system has no connectivity to a higher-level system, don't need to protect or do anything further

- Dave Pierce willing to put together a working paper on this

Chapter 2 – Regulatory Considerations to include 2.1 IUEI

- Dan Johnson wrote a lot of this, do we want to sign him up again? Reuse material from ARAC report?
- Content would be definition + examples
- Dave Pierce – this section needs to appear more informational than directive
- Why is it under Regulatory considerations and involvement? Whether or not you have to show protections and how much
- Stefan Schmidt– Level Of Involvement (LOI) means something different, do we want to get into it?

Type design and STC, 2.3

- Does text about major criteria and examples go here, appendix, or both?
- Dave Pierce – compare proposed text to what is in the ARAC report to check

Siobvan Nyikos assigned 2.5 Considerations for Continued Airworthiness Security, makes sense that DAH (e.g. Boeing) be assigned this, work with colleagues to get proper content
Sections:
2.5.1 Discuss relationship with DO-355
2.5.2 Security environment monitoring (external)
2.5.3 Security effectiveness monitoring (internal)
2.5.4 Triggers for re-assessment, response
WG-72 will work this as well from their perspective, Jean-Paul?

Item #10 in the TOR is different from the one in the ARAC report

- 10 got misinterpreted, TOR discusses trustworthiness and ARAC report discusses sharing SSI data
- Section is 2.6 Trust considerations in the security environment

WG-72 has a working draft of ED-203A where they have dropped proposed text from working papers into the appropriate sections

2.3.2 Vulnerability Assessment and Classification – Dan Johnson

- Dan Johnson has action to "find a home" for this material
- Reviewed Bernie Newman's working paper, 2.2.1
- Going through comments spreadsheet (see spreadsheet for details)
- Threat conditions vs. scenarios discussion
- WG-72 talking through their position internally
- They have an example that covers all three levels from aircraft to item level

Discussed meeting locations for 2017

- February in Phoenix – better facilities, no escort
- March in Brussels, not confirmed yet
- May in DC – rooms reserved (follow up after Plenary 30 – location may change again due to budget constraints)

Stefan Schmidt proposed putting due dates for working papers on schedule to keep us to task

April 28, 2017 – decision point for US federal gov't, need to get all trips, funding, etc. in before then

Afternoon plan – look at logging and major criteria working papers

End joint session, begin SC-216 plenary

Chapter 6.2 CONOPS for Logging and Audit working paper review, Romuald Salgues (Airbus)

- Varun Khanna – data format needs to be close so that different tools can do the analysis on the same data
- Phil Watson – let ARINC decide, see relevant material, ARINC 852
- Data format depends on architecture
- Will there be real time monitoring?
- Security event does not necessarily translate to a safety event
- Security events need to examined to determine if safety is affected
- Chuck Royalty - Log when authentication succeeds, fails, and if there is a violation of security rules (aligns with FAA issue papers for network security)
- Want Chuck Royalty to participate in joint session tomorrow morning

CONOPS for once airplane leaves OEM

- Siobvan Nyikos and Varun Khanna – DAH doesn't report failures, that happens with the operator and airlines maintenance
- Chuck Royalty – DAH supports investigations, there are corner cases where DAH reports failures
- Changed bullet to make it clear that most of the time, DAH support investigations and only in some cases has the information to report

Definition of logging

- Varun Khanna – logging is not a security measure, it simply records what happened
- Dave Pierce doesn't like the term "reactive"
- Chuck Royalty – reactive means it logs but does not react to events logged, goes back to discussion on how we don't do anything with the logs
- Bernie Newman – for CONOPS, say what logging is, not what it isn't

Role of law enforcement

- Chuck Royalty – systems and records may contain evidence of unlawful activity
- Mitchell Trope– careful of wording, don't want to imply that law enforcement should be audited by FAA
- Revised Chuck Royalty's wording so that it's a heads' up that another agency may want to see the records, but we are not opening ourselves up or implying a new audit requirement

Siobvan Nyikos – take out "case by case", if an e-enabled aircraft goes by special conditions and issue papers, then they do logging because that is called out in the issue papers

IFE case

- Note about applicant choosing to log even if there aren't security requirements (e.g. IFE) – is note necessary? Don't want to imply that it is necessary

- Changing note – For systems that don't require logging, an applicant may choose to implement security logging as desired for business needs…
- Bernie Newman – use note and delete in CONOPS #4, if it is truly a note and doesn't belong in CONOPS, ask WG-72 tomorrow if that was their intent
- Dave Pierce – as time goes on, you will get a better idea of what needs to be logged

Bernie Newman looking at AC 119-1, mentions logging

For 2.4.1 DAH responsibilities, STC and TSO can be DAH and are included

Standards came up again, it is desirable to have same or similar format of log data, but might not be possible due to aircraft architectures, up to ARINC 852 to sort out

Objectives of logging
- Sections 6 and 7 of ARINC 852 provide guidance to support operator and/or DAH
- What are the objectives of the data?
- Bernie Newman pulled up ARINC 852 – it says not only is airline responsible for collection of log data, but they are responsible for investigation as well
- New draft of ARINC 852 in January 2017, check back then

Finished providing markups and comments for 6.2

Reviewed Siobvan Nyikos' working paper for major criteria (change impact analysis, STC, etc.), does material belong in Appendix, STC section, or both?

Reviewed Siobvan Nyikos' cert evidence paper

Day 3

Joint SC-216 and WG-72 meeting

WG-72 went through logging paper this morning internally, plan to go over logging paper jointly
- Security event logging is different from other logging on the airplane
- Might be necessary to separate security logs from other logs depending on threats and events
- Agreement that issue is that no one currently looks at the logs
- Chuck Royalty - Use logging function in support of airplane operations, if someone is required to use logs in ICA, then they will look at the logs in a timely manner
- Varun Khanna – security or maintenance logs? If maintenance logs included, we are already requiring them and incorporating them into airworthiness
- Romuald will update table by next meeting
- Bernie Newman looked at sections 6 and 7 of ARINC 852, section 6 talked about operator looking at logs rather than providing to DAH, will section 6 and 7 remain as is putting the burden on operator? Anyone involved enough to know? no
- Michel Messerschmidt – wait and see next revision

Looked at acceptability next
- "The evaluation of likelihood is always dependent on attack properties for which no assurance statements can be made" – SC-216 members don't agree with that statement

- Looked at tables in ARAC report as well as working paper
- Bernie Newman – at ARAC, discussion of could likelihood of attack be looked at as a different way of effectiveness of security measure, both viable ways and different perspectives of same topic
- Reconcile by saying both perspectives are equivalent?
- Vertical axis only difference between tables, both tables can help you arrive at same conclusion and risk acceptability
- Need an explanation of diagram and something to show the correlation
- Larry Hannert – we didn't need these tables for software, why do we need them here? Tables creating controversy

Moved into level of threat discussion

- Shohreh Safaria – table 2-1 shows that for Minor and None, risk is "Not Acceptable", conflicts because we assumed that minor assets don't require protection?
- Discussed consideration of nation state threats

End joint session, begin SC-216 plenary

Internal discussion of risk acceptability

- Bernie Newman - Need complete working paper from Patrick Morrissey before we can go much further on risk acceptability, he wasn't able to make it to this meeting
- So far, identified contradictions and questions, but not in working paper format or inclusive of proposed solutions
- Chuck Royalty – want to get more specific about type of security, Michel Messerschmidt seems to be alluding to crypto and key based in some of the text
- Bernie Newman comparing DO-356 to ED-203
- DO-356 – likelihood includes effectiveness of controls, trustworthiness, etc.
- Further, ED-203 effectiveness includes more factors
- All of this rolls into likelihood
- Michel Messerschmidt made harmonization working paper out of section 2.7, didn't post, but sent to Bernie Newman for review
- Review 2.7, use comments as seed for whichever SC-216 member is going to take it on from our perspective

Figure 2.2-2

- DO-356 has text that supports figure, relation of effectiveness and level of threat, but that text is not in ED-203
- Context / supporting text is needed, not even sure what the figure means
- Phillipe from WG-72 most likely created the figure
- Change figure? Delete since text in DO-356 conveys same message? (FAA vote)
- Environment is security environment, architecture is security perimeter assuming he didn't create something new
- SC-216 recommends deleting figure 2.2-2 unless we can get clarification added from Phillipe

Likelihood and difficulty of attack

- Larry Hannert – term "difficulty of attack", how does it fit in, how is it defined and measured
- Carnegie Melon person said attack either happens or it doesn't, they don't take into consideration the difficulty

- The likelihood that a threat scenario can be success completed – true statement out of this
- Chuck Royalty – doesn't like "difficulty of attack", do I cover all possible attacks or not?

Effectiveness and classification of assets

- Table 2-1 acceptable relationship between severity of effect and effectiveness objective, asterisk by catastrophic & very high, only acceptable if there is no single point failure for this DAL
- Mentioned earlier, minor & none is unacceptable, but that conflicts with ARAC committee suggestion that we don't need to protect minor and no effect assets with no internal connectivity to systems with major or higher, including if they have external connections
- Phil Watson emailed text to go along with table and address minor & none issue
- Unacceptable if and only if the threat scenario's chain of protection involves a system with a hazard classification of major or above, either directly or indirectly via a system with hazard classification of major or above
- Hazard classification = threat condition severity of effect
- Reviewing text "Minor and lower hazard classification system have the following exceptions to the above…" to ensure we aren't doing anything in violation
- Bernie Newman working with Michel Messerschmidt on 2.7 working paper and table, give Bernie Newman input on which table to use

Looked at Dave Pierce's section 3.1 and comments, see comments spreadsheet for more details

Discussed Siobvan Nyikos' concerns re: Chapter 5 and closing out concerns

- Stick to ARINC 811 or add other examples of classifying into domains? Siobvan Nyikos to ask Airbus if there is any other documented way to organize by domain, does Airbus use something other than ARINC 811? Boeing uses ARINC 811
- Defense in depth subsection - Siobvan Nyikos to work with Chuck Royalty offline, he has ideas on how to address

<u>Day 4</u>

Joint SC-216 and WG-72 session

Siobvan Nyikos asked her questions re: Chapter 5, is there a document other than ARINC 811 that defines domains that Airbus uses?

- Jean-Paul Moreaux - ARINC 664 Part 5 (provided info afterwards via email)
- A lot of ARINC 811 came from 664, but there are some misinterpretations
- Not a fixed set of functionality
- Look at 202A scope for guidance
- ARINC 811 domains is the special case model, not the rule
- Siobvan Nyikos also asked if WG-72 had additional guidance on defense in depth
- Michel Messerschmidt said he could provide some in the new year

Dave Pierce brought up security assurance and how we should approach it, Bernie Newman and Michel Messerschmidt can put working paper together

Went through action items

For Phoenix meeting February 6-10, 2017, would be nice to have more detailed agenda with time slots and discussion periods for working papers, make week flow better

Looked at section 4.2 and tables

- Varun Khanna - Compiler bugs – not unique to security, applies to system in general
- Need to get to 95% solution
- John Angermayer on phone now, disagrees and still wants to go to that granularity
- Reviewed matrix – software planning process
- Don't need to have several software teams doing the same thing
- Extend code review to level D?
- Chuck Royalty – nothing saying you can't use procured software at level D or E for which you don't have code
- John Angermayer – if we require source code at level D, dramatic change to DO-178
- Chuck Royalty – compensate for not having the code by having different approach to testing, looking at CVEs as COTS has lots of info, etc.
- Varun Khanna – assume that COTS code can fail and that it is "architecturally mitigated"
- Chuck Royalty – identify security issue as opposed to safety issue, in particular unintended function, is it harmful unintended function?
- Bernie Newman – level D, we are willing to live with what could go wrong because it is minor

Dataloader case

- Michel Messerschmidt – what about dataloader? That is the type of code they are looking at right now
- John Angermayer – dataloaders are D because the software that actually runs them is at a higher level and can tell if the dataloader is functioning correctly
- Varun Khanna - End system responsible for load coming into it

Phil Watson – statement implies if there is no impact to security, steps are not applicable, analysis to determine which system have impact security?

Stefan Schmidt– analysis is part of security process, even if initial analysis, safety assessment done from DAL E to DAL A because you need to determine, FHA as opposed to P/ANSSA or Airbus equivalent, security always involved in initial evaluation and then you determine how far the certification activities go

No joint session the next day (Friday)

End joint session, begin SC-216 plenary

Looking at chapter 4 security assurance again

- Jumping between independent and supplemental security evaluation this morning
- We want supplemental that builds on safety that already exists
- Airbus wants independent security evaluation
- Problem – implies two code reviews, two sets of test, etc.
- Both methods will be in both documents as documents need to be identical, the cert authority will decide which one the DAH needs to use

John Angermayer – may need to split validation and verification data into two parts, different SCC levels

Term "system security architecture" – how is it different from just plain architecture? Looking at architecture for security and safety elements

- Creating evidence, not a brand new architecture
- System security architecture and system safety architecture are referenced in matrix, but they should be the same thing
- DO-326A says system security architecture

Process objectives for item development table

- Varun Khanna – term "functional" is too broad, security functional more appropriate, does this pertain to ANSOG guidance?
- If it pertains to security, specify security functional, though it can be taken care of via system functions

Should we implement security controls at DAL E discussion (had same discussion in September)

- Varun Khanna – don't want to take cert credit, would be OK with "security demonstration" or another term
- Bernie Newman brought up discussion with Cyrille Rosay in September
- Cyrille Rosay – DAL E handled via system level (system provides protection for item at Level E)
- Dan Johnson – most DAL E COTS are actually handled at item level
- Mitchell Trope– if we want to do this for business purposes, that's OK, but it belongs in a different document with different scope
- Dave Pierce – should be handled during assets protection discussion
- Chuck Royalty – part of your system functionality with respect to security, need to demonstrate functionality

Varun Khanna and Chuck Royalty don't like SCC term, Chuck Royalty said we can add asterisks, notes, etc. to clarify this in the table

Chuck Royalty – if you leave the column blank, you force systems to be level D or higher for security

Plan for afternoon – look at independent table and trustworthiness levels in preparation for next meeting

Supplement (cont'd)

- Back to discussion about COTS – we would like to have access to the code, but in reality we won't
- John Angermayer – TQL doesn't have to do with access to source code
- Chuck Royalty – point is to supplement other development process, guidance to answer questions, this is appropriate for most situations (COTS tool qualification at level D)
- John Angermayer - DO-178C has the TQL level diagram, can point to it or pull it in if needed
- Chuck Royalty - If you are using the tools in this way, use TQL 5, but still need configuration control
- John Angermayer – not onboard with using TQL 5

- Dave Pierce - Determination of TQL level should be left to DO-178, we don't want to have different guidance, we want to leave it up to one, should we "kill" table?
- Bernie Newman – replace rather than remove in case we need something specific to security
- Independent
- Phil Watson – not clear on SAL for a target concept, table 4-2, why are all the SAL for targets 1 and then there are different levels for one security measure and another security measure?
- Dave Pierce - WG-72 wanted to independently assign security levels like firewalls, but still doesn't understand SAL for target, record as comment to WG-72 to explain

Soon there will be official direction that EASA certifies for Europe, FAA certifies for US, and you don't need to worry about the other agency retaining for compliance or turning in cert evidence to another authority. In other words, if FAA approves, EASA delegates that approval of the FAA

PSec vs. PSecAC, John Angermayer – need to include plan reviews, objective for review of plans

Patch levels and mod numbers aren't equivalent, different operational concepts

- Patches only allowed in development, once software is black label, no more patches, needs to be an actual part number roll
- This is for Level A, B, and C systems / software
- See comments / notes against table for further details

Varun Khanna - "Derived requirements are validated against security risk assessments" – what does this mean? Security assessment will change, not derived requirements

- How much power do we security have? How much do we drive security requirements and get them implemented vs. adding security in later to a design we have to live with?
- Appears to disagree with DO-178 and say security is more important than safety
- Chuck Royalty – they are trying to disentangle SAL from DAL

John Angermayer to Chuck Royalty – do you consider fuzz testing equivalent to robustness testing? Chuck Royalty - No, fuzz testing is a way to do robustness testing, don't want to force someone to do fuzz testing

Term "refutation", refers to negative testing

Trustworthiness

- Siobvan Nyikos - ARAC report presents both approaches but no direction, both approaches in harmonized document?
- Phil Watson – recent news stories make you rethink who is to be considered trusted

Showed schedule one more time (highlights below):

December 12-16, 2016	Joint WG72 (Cologne EASA) / SC216 (DC RTCA) + Plenary
February 6-10, 2017	Joint WG72 / SC-216 Plenary (Phoenix)
March 27-31, 2017	Joint WG72 / SC-216 Plenary (Brussels)
May 15-19, 2017	Joint WG72 / SC-216 Plenary (Seattle or DC)
June 26, 2017	DO-356A/ED203A Compiled Draft distributed to SC-216/WG72
July 24 - 28, 2017	Joint WG72 / SC-216 Plenary Disposition (Hamburg)
August 18, 2017	DO-356A FRAC Ready version to RTCA/EUROCAE PM
September 1, 2017	DO-356A/ED203A Begins FRAC/OC

October 20, 2017	DO-356A/ED203A FRAC/OC Review Period complete
November 1, 2017	FRAC Initial disposition by Authors distributed to SC-216 / WG72
November 6-10, 2017	Initial DO-356A/ED203A FRAC / OC Disposition Meeting (Paris)
December 11-15, 2017	Final DO-356A/ED203A FRAC / OC Disposition Meeting (DC)
December 16, 2017	DO-356A/ED203A FRAC Comments dispositioned
December 31, 2017	DO-356A/ED203A final version to RTCA/EUROCAE PM

Day 5 cancelled

/s/
Siobvan Nyikos
Secretary, SC-216
CERTIFIED as a true and accurate summary of the meeting

/s/
David Pierce
Co-Chairman, SC-216

/s/
Daniel Johnson
Co-Chairman, SC-216