RTCA Paper No. 323-16/SC216-063
November 29, 2016

Summary of the Twenty-Ninth Meeting
Special Committee 216
Aeronautical Systems Security

DATE: September 19-23, 2016

PLACE: General Aviation Manufacturers Association (GAMA), Inc.
1400 K St NW #801
Washington, DC 20005

The Committee wishes to thank GAMA for hosting this meeting.

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

ATTENDEES:

SC-216 Co-Chairs

Daniel Johnson	Honeywell International, Inc.
David Pierce	GE Aviation

SC-216 Secretary

Derek Schatz	Boeing Commercial Airplanes

Designated Federal Official:

Varun Khanna	Federal Aviation Administration (FAA)

Members attended:

Siobvan Nyikos	Boeing Commercial Airplanes
Bernie Newman	Astronautics Corporation of America
Dinkar Mokadam	AFA-CWA
Patrick Morrissey	Rockwell Collins, Inc.
Mitchell Trope	Garmin Ltd.
Phil Watson	Panasonic Avionics
Tom Phan	Federal Aviation Administration
Steve Bates	Panasonic Avionics

Members attended by phone:

WG-72	EUROCAE

John Flores	Federal Aviation Administration
Larry Hannert	LCH Engineering
Chuck Royalty	R5Y Consulting
Shohreh Safarian	Federal Aviation Administration
Tong Vu	Federal Aviation Administration
Michael Avari	Cigital
John Angermayer (last day)	MITRE

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 May 23, 2016. Attendance is open to the interested public. 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 Chairs 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

Final ARAC ASISP report approved by FAA, but SC-216 does not have access to a copy of the report yet

- ARAC is concerned someone is talking to the press
- Ultimately, it will be part of public domain, in the meantime, it needs to be available to working committee

Go through action items together with WG-72 – see action item log for status and details

- Security (penetration) testing – what is the stopping criteria for negative testing? Dan Johnson - Balance between detail and abstract because there are different means of compliance.
    - Varun– there needs to be some stop criteria otherwise you will never be done, at some point it has to be good enough so that applicant isn't out of business
    - Jean-Paul working on this from WG-72 end, he can send proposed wording or stop criteria to Varun, and Varun can farm it out to whoever needs to see it in the FAA
- Need to ensure working papers and proposed text are "manufacturer agnostic"
- Planning real-time working paper reviews during this week's meetings
- Dan sent scoping statement to Varun for FAA, will send to EASA as well
- Move schedule discussion to Thursday morning since people are leaving early Friday

Went through proposed table of contents, made clarifications and additional assignments, specified which items came out of ARAC where we are awaiting final report, assigned a corresponding WG-72 person to items where it made sense to ensure draft was pre-reviewed before going out for general comment

- Varun – STC examples going through Major/Minor criteria – make sure to review
- Dave– 2.6 Trust Considerations – make sure to review
- Dan taking over 3.1 Risk Assessment Framework – make sure to review
- 4.9 assurance for layered protection will need to agree with 5.4 for defense-in-depth, assigned to Chuck
- Patrick working on effectiveness vs. development assurance, will fit in 4.1 characterizing effectiveness, this is in DO-356 but not ED-203
- Revise threat condition flow chart – put flow chart figures in text or flow chart?
- Dan to post updated TOC

Out brief on what WG-72 did this morning, what would WG-72 like us to work on this afternoon?

WG-72 went through their action list and TOC

What does SC-216 want WG-72 to do tomorrow morning before we do our joint meeting? Dave proposed discussing operating rhythm for how many times the groups need to meet, go through papers they haven't had a chance to review yet

End joint meeting, begin SC-216 working meeting

Looked at consolidated WG-72 comments on DO-356 prior to harmonized TOC, Dan took action to map to current DO-356A sections and send to authors

Bernie and Siobvan already started working comments that belong to their sections

Start internal SC-216 review of working papers, starting with Bernie's 3.3 Threat Condition Identification and Evaluation

- Remove "safety margin" from this section but it is still a valid term to define
- Put flow chart in appendix, but it still needs to be fixed
- Scope – only mention part 25, everything else is open, scoping statement will be tailored from our (SC-216) perspective
- Discussion of CIA and whether or not we want to entertain that there could be more security attributes, decided to leave it as "typically"
- Discussion of flight crew vs. occupants. Technically, everyone on the plane is an occupant. The categories are flight crew, crew, supernumerary, passengers, etc. Is it possible for a security/safety event to affect one category and not another? Or have a different level of effect? Yes
- Vulnerability Dossier = collection of vulnerabilities found

Reviewed 3.5, Siobvan presented, see comments for summary of discussion

Additional comments in HWP_comments from WG-72

Reviewed 3.6

- Looked at risk acceptability matrices
- Harmonize two matrices or have two matrices that coexist?
- Effectiveness is whether the security measures are free of errors and defects
- 2 risks
    - Ones you don't know – use assurance to reduce level of defect
    - Ones you know – other parts of the process

Reviewed 4.8.2

<u>Day 2</u>

Began with Joint SC-216 & WG-72 meeting

Summarized what we did at our respective meetings before the joint session, looked at flow chart from ED-203

- Romuald - This is not the final flow chart, flow chart is useful in supporting audit
- Dan – how in the document do you show how you followed the process, having the flow chart is not enough, flow charts do not make sense when you are talking about the contents of an activity
- Varun – this is written for requirements, not audit, so audit argument for the flow chart won't work
- Dan - Is the final list of threat conditions complete? Flow chart does not ensure completeness. Put as an example in the appendix
- Bernie volunteered to do a high level flow chart (to be put in appendix)

Scope is Part 25

Eliminate use of system, only say aircraft system vs. system when applicable, possibly use Chuck's new term, "element"?

Discussed ED-203 comments on Bernie's paper 3.3

- Discussion yesterday if there is a threat condition that can affect the passengers, but not crew (and vice versa)
- Usefulness of examples discussion again

Discussed Siobvan's section 3.5 and the response to comments / edits to working paper from day before – WG-72 is good with everything, that chapter is more or less approved/complete

Discussed ED-203 comments on Chuck's paper 4.8.2, may need to add examples to the text

End joint session, begin SC-216 working session

Looking at a new paper – Dave's section 3.1

- Steps for determining security figure (2-6 from DO-356)
    - Group agrees it is a good diagram, keep it
    - Figure 2-7 seems to be a continuation of it
- What is meant by external threats (as opposed to internal)?
    - Separate FAA issue papers for internal vs. external
    - External threats are external to the skin of the airplane
    - What about systems? An external threat to a system could be internal to the airplane. How to define?
- Went through additional comments
    - Typo or omit on "national" from table on examples of trustworthiness standards, varies by national agency, generated discussion on how this actually works
    - External populations will be in final glossary, generated discussion on who the comments are coming from, FRAC is public, working group is private
    - Nested assets completely different from defense in depth

Chapter 5 next

<u>Day 3</u>

Joint SC-216 and WG-72 meeting

Discussed how to manage comments, authors have responsibility to collect and track comments in a spreadsheet, reviewers have responsibility to provide comments to authors and ensure they are addressed to their satisfaction

Better to have each author handle their own comments as one universal comments spreadsheet would be difficult to manage

WG-72 not ready to review FAA-EASA letter yet

Reviewed 3.1 (scope) and WG-72 comments + responses

Correction from yesterday, varies by national agency is changing to varies by regulatory agency in Table 2-2, regulatory more correct

Reviewed part of chapter 5, assigned to Siobvan

- WG-72 still wants (ARINC 811) functional domain discussion in appendix as an example, not in chapter 5 text
- SC-216 agrees to move only the section on ARINC 811 domains to later section in chapter 5 or appendix
- Subsections of 5.1 should actually say "Network Security Domain…"
- Discussion of bullet on domain security policy, relationship between requirements and assessment
- If we change "Domain security policy" to "Domain security rules and requirements", do we need to revise definition below, where policy is defined?
- This is one way, not the way or the only way, might need to state this up front
- DO-326A talks about interactions, WG-72 wants the harmonized 356/203 document to discuss these as well, carry wording forward? Interactions between disciplines, steps, etc.
- Dan said we could argue that we are not required to change the text because it is not one of the 10 tasks from ARAC. Harmonization is our (SC-216) own desire, not ARAC's

End joint session, begin SC-216 working session

SC-216 agreed to reconvene a little earlier the next day, 8:30 Eastern

Start with schedule discussion

- Next meeting and final of the year – December 12-16, 2016
- February meeting to be in Clearwater, Florida or Phoenix, Arizona
- Changed April 2017 meeting to March 27-31, 2017
- See updated schedule power point for all updates

Reviewed rest of chapter 5 comments (see spreadsheet and updated document)

Reviewed Dan's working paper

Day 4

Joint SC-216 and WG-72 session

Discussed schedule, made some date and location changes (see schedule slide)

Discussed scope statement

Discussed best day/time to have the weekly joint WG-72 and SC-216 call, currently Tuesdays at 7, changing to Wednesdays at 7?

Reviewed working paper on Chapter 4 Security Assurance, "Independent security organization is established"

- Change independent to adequate, don't force a company to outsource security, only required with QA
- Change established to identified, no need to establish what already exists
- Better yet, take out wording, why are we (security) doing something safety doesn't have to do?
- Doesn't belong in security objectives

Discussion of waterfalls and feedback loops in process

Reviewed assurance tables in Appendix

- Discussed refutation
- Can't have one-to-one between security guidance and safety in DO-178
- Dan – system vs. item makes a difference, for example, software is an item until it is installed and can function, then it is part of a system
- Monolithic? WG-72 term, means consistent between risk assessment phases
- Verification plan vs. test plan? Same or different?

No joint session the next day (Friday)

End joint session, begin SC-216 working session

SC-216 needs to agree on assurance tables internally before bringing this to a joint session again

- Need to stay away from silo-ization
- Another instance where we need two methods

Penetration test discussion

- Chuck – vulnerability testing isn't pen testing
- Dan – if someone can get access, assume they can and will exploit, don't need to demonstrate exploitation
- Phil – Pen testing, negative testing – when do you know when to stop? Different for closed versus open systems (Panasonic is concerned about their open systems)
- Red teaming vs. having full knowledge of airplane (black box vs. white box testing)
- Varun – definition of pen testing too broad
- Dave - EASA has hard stopping criteria for pen test
- Mitch - Pen testing is a good practice and should be a part of development, but not part of the critical path of certification

DAL E+ cert cred came up again, level E code that we are taking credit for in security

Item table, not system table (revert back to software example)

DO-356 to date has not committed to using a SAL, DAL, etc., WG-72 wants SAL

Reviewed Bernie's changes based on yesterday's discussion

Bernie has wording that might be more appropriate to include/address in 3.5 security measure characterization

Reviewed updated chapter 5 again

- Added wording to 5.1 per WG-72 comment
- Edited enclave figure, original figure was trying to show too much, removed VPN
- Dan checked updated WG-72 spreadsheet, no new comments for chapter 5

Larry discussing WG-72 perspectives since he is a consulting for Airbus
No meeting tomorrow (Friday), ran out of topics and working papers to review

Day 5 cancelled

/s/
Siobvan Nyikos, taking over for Derek Schatz
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