EUR 142-18 / WG72-110
RTCA 120-18/SC216-083 St Denis and Washington, 24 April 2018

Summary of the Meeting of RTCA Special Committee 216 (Meeting #39)
EUROCAE Working Group 72 (Meeting #51)
Aeronautical Systems Security

**DATE:** Apr 9th to 13th, 2018

**PLACE:** RTCA Washington

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

**ATTENDEES:**

| | | | | | April 2018 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Name** | **First Name** | **Company** | **SC-216** | **WG-72** | **9** | **10** | **11** | **12** | **13** |
| Allen | Severn | Boeing | X | | T | | | | |
| Angemayer | John | MITRE | X | | T | P | T | T | T |
| Ayari | Mehdi | Airbus | | X | P | P | P | P | P |
| Bates | Steve | Panasonic Avionics Corporation | X | | P | P | P | P | P |
| Call | Martin | Boeing | X | | T | T | T | T | T |
| Descarques | Gilles | Thales | | X | | | | | T |
| Flores | John | FAA | X | | T | T | T | T | |
| Frietas | Joacy | ANAC | X | | | T | | | |
| Fuilla | Patricia | Apsys for Airbus | | X | T | T | | T | T |
| Gariou | Raoufou | Transport Canada | X | | T | T | T | T | T |
| Gauthé | Armelle | Apsys for Airbus | | X | P | P | P | P | P |
| Gobbo | Giles | Airbus | | X | P | P | P | P | P |
| Goodchild | Clive | BAE Systems | | X | T | T | T | | T |
| Hahn | Edward | ALPA | X | | P | P | P | P | P |
| Hannert | Larry | LCH | X | | T | T | T | T | T |
| Hennig | Jens | GAMMA | X | | P | P | P | P | P |
| Haury | Christian | SAFRAN | | X | T | T | T | T | T |
| Henrique de | Claudio | Embraer | | X | P | P | P | P | P |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Castro | | | | | | | | | |
| Hoffman | Brian | ALPA | X | | T | T | T | T | T |
| Hofmann | Karan | RTCA | X | | P | T | T | | P |
| Hrubesz | Marek | Department of National Defence of Canada | X | | T | T | T | T | T |
| Jean | Chris | George Washington University | | | P | P | P | P | P |
| Johnson | Dan | Honeywell | X | | | | | | |
| Kelly | Mark | Esterline AVISTA | X | | P | P | P | P | P |
| Khanna | Varun | FAA | X | | P | P | P | P | P |
| Leonardon | Laurent | Rockwell Collins | | | | | | | T |
| Marchand | Cyril | Thales | | X | P | P | P | P | P |
| Marquis | Philippe | Dassault | | X | P | P | P | P | P |
| Masri | Sam | Honeywell | X | | P | P | P | P | P |
| Messerschmidt | Michel | Airbus | | X | P | P | P | P | P |
| Monot | Thomas | SAFRAN | | X | T | T | T | | |
| Morrison | Rebecca | RTCA | X | | | T | T | T | |
| Morrissey | Patrick | Rockwell Collins | X | | P | P | P | P | P |
| Nori | Ravi | Teledyne Controls | X | | T | T | T | T | T |
| Nguyen | Daniel | Boeing Test & Evaluation | X | | | P | P | P | P |
| Nyikos | Siobvan Megan | Boeing Commercial Airplanes | X | | | P | P | P | P |
| Pacher | Martin | European Cockpit Association | | X | | | | | |
| Pierce | Dave | GE | X | | P | P | P | P | P |
| Rambert | Steve | FAA | X | | P | P | P | P | P |
| Rosay | Cyrille | EASA | | X | | | T | T | T |
| Rosenberg | Silvia | ANAC | | X | | | T | T | |
| Royalty | Chuck | Aerospace Systems Cyber Security | X | | T | T | T | T | T |
| Salgues | Romuald | Airbus | X | | P | P | P | P | P |
| Sampigethaya | Krishna | UTRC | X | | P | P | P | P | P |
| Schwindt | Stefan | GE | | X | T | T | T | T | T |
| Secen | Al | RTCA | X | | | | P | | |
| Shuang | Zhang | Avic | X | | | | | | |
| Skaves | Peter | FAA | X | | T | T | T | T | T |
| Tinney | Tim | AAB | | | T | T | T | T | T |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Trope | Mitchell | Garmin | | X | P | P | P | P | P |
| Verna | Brian | FAA | X | | P | P | P | P | P |
| Groote | Anna | EUROCAE | | | | | T | | |
| Waheed | Mohamed | Aviage Systems | X | | P | P | P | P | P |
| Watson | Philip | Panasonic Avionics Corporation | X | | P | P | P | P | P |

P In Person, T telephone

# 1 Executive Summary

During this plenary, both dissenting opinions were resolved, and all non-editorial comments were addressed per RTCA and EUROCAE process. On the last day, SC-216 and WG-72 voted unanimously yes to publishing DO-356A/ED-203A. Expected publication will be late June 2018.

1. Day One
    a. Status of the comment resolution and the process for the two dissenting opinion documents
    b. Initial discussion on the dissenting opinions comments
    c. Review and comment closure for Security Assurance and Risk Assessment
2. Day Two
    a. Review and closure of comments associated with Objectives, Document scope, Example Methods, Certification, Assets, Trustworthiness, Risk acceptability, Document Consistency, Security scope, Architecture, External, Level of Threat, Terms and Definitions
3. Day Three
    a. Discussion on the consensus exercise
    b. Review and discussion in the Panasonic dissenting opinion and formulation of a solution that when implemented in the draft will result in the DOI being withdrawn
    c. Review of Measures
    d. Start of the review of the second dissenting opinion document
4. Day Four
    a. Second dissenting paper resolved and withdrawn final NC resolved and closed
    b. All high comments now resolved except one
5. Day Five
    a. Review, resolution and closure of Final High, Medium and low comments and closure of some of the editorial comments
    b. Consensus process for publication of the document
        i. Unanimous yes vote in room!
        ii. Unanimous yes vote on the phone/webex!
        iii. Unanimous opinion to publish document

# 2 Monday, April 9, 2018

1. Welcome and Administrative Statements/Remarks – Karan H/Anna vG 9:00am
    a. Opening Remarks from Dave Pierce
    b. Varun reads out the official FACA opening remarks
    c. Open remarks from Karan – RTCA proprietary policy and membership policy as well as EUROCAE IPR Policy call and membership policy
2. FAA/EASA Remarks and Regulatory Status –Varun K/Cyrille R
    a. Varun will provide comments tomorrow after discussions with the FAA encourages a single path
3. SC-216 March Minutes Review and Approval – Dave P
    a. Minutes are on the RTCA site
4. Agenda – Dave P
5. FRAC/OC Comment Period Overall Status – Dave P/Michel M
    a. Thank you to everybody and the group has worked through nearly 2300 comments in the last few months
    b. 1334 comments - 393 closed or accepted
    c. Michel provided an update and said that further progress had been made over the weekend

d. Dave Pierce – The new and "assigned" need to be a priority, and then went through the process for the work and subsequent updates after the meeting, looking for volunteers for proof reading
e. May 8th document has go to RTCA and EUROCAE in time for RTCA PMC on June 21, 2018
f. All non-editorial comments need to be resolved this week
g. Two dissenting opinion papers have been received, it had to be presented to the chair by last Thursday. Both sides will then present to the PMC and then PMC will listen to both sides and then pick which side, dissenting opinion and rebuttal included. For EUROCAE both sides present to the council and the council decides which direction the document will go and then makes a decision one or way other
h. Sidebar will be conducted with EUROCAE to see what happens with a dissenting opinion for a harmonised document

6. BREAK
7. Panasonic Dissenting Opinion – Dave P/Steve B
    a. Security measures for DAL E equipment, and that the use of security measures with any level of assurance on DAL E equipment is not acceptable
    b. Possible solution proposed to address assurance of underlying system and the security assurance proposed
    c. Include additional test in architecture session
    d. He is opposed to the lack of guidance for independence and isolation
    e. Stefan – proposal Stefan did address some of this but there is still some disagreement
    f. Philippe Marquis – definition is independence and isolation is only between two security measures
    g. Philippe – relates to the common mode action, so that text needs to be discussed
    h. A review was then con=ducted on Steve's text
    i. Romuald does not consider this to be a valid point – as an OEM needs security applied where it is required and is an applicant solution and should not be described in the guidance material, and this is two prescriptive
    j. Varun – issue is you are adding a security control to a level E system because you want it, and FAA won't acknowledge it. The proposal of independence, if you separate the required security controls its good
    k. Steve – you can't do this without independence and isolation of the function that you have added
    l. Varun – Level E goes on system for two cases only – don't catch fire and can't affect other systems, and unless you can segregate it
    m. Chuck – Varun comments address his thoughts
    n. Martin Call – Every time there is a change to a non-essential system, there is a check for impact for safety, and the applicant has that responsibility to determine the change impact, His concern with the re-write – is that this will mean that the security measure would need to be Level D
    o. Varun – you have to show that the security measure works, and SAL does not tell me anything
    p. Martin – Point of introducing SAL was to provide assurance for security
    q. Romuald – He understands the Panasonic solution, but this is not the only solution. It is up to the applicant to demonstrate the assurance

r. Varun – does not have a problem with another way of doing it, the problem he has is where Martin is going to come from, where are the security requirements coming from, it is all 178 based
s. Stefan – We should keep the agenda and not get into the details, some should be clarified with proposal from other comments
t. Steve – you're putting a security measure in for safety
u. Michel – should be put on the workspace so that it can be reviewed on Wednesday
v. Martin – Even today DAL E systems have requirements that are verified, what we are proposing here that that is a process called SAL where requirements are continued to be verified which is outside DO-178
w. Stefan – He can see the concerns – but can't see why it is a dissenting opinion, as the AMC could clarify this
x. Dave – If we had some agreement from the regulatory authority
y. Varun – so your punting the problem to us
z. Dave P – no we have not decided anything yet, different views on how a system architecture should be implemented. He does not want security process on an island. If it is to be independent, it needs to do all the other safety processes

8. Aerosystems Security Dissenting Opinion – Dave P/Chuck R
    a. Overview of the view
        i. Dissociation between vulnerabilities and errors and what DAL means and what SAL means
        ii. Does not address safety hazards in the same treatment – and chapter 4 goes off to an independent view
        iii. SALS are not mapped to DAL, and the level of rigour is not the same
        iv. Chuck
            1. Threat conditions should be expressed as in Section 3 and that is ignored later on in chapter 4
            2. He is advocating that the safety impact is reflected in the design
            3. He is proposing two changes to chapter four and the tables
    b. Stefan – Then this also requires a change to DO-326A as we don't have a feedback to safety process in there as well
    c. Chuck – There is a lot of diversity and in this document, it is getting worse and not better,
    d. Romuald – Would like to remind that as an airframer we have already certified A380 and 350 with solutions that are different from both dissenting papers, and the applicant needs that freedom, and hence only need security specific activities
    e. Martin – DO-178 has been around a long time, and within each company people have different understandings of what 178 means, so we will never get a document where everybody will get to the same conclusion. If we have a threat condition that is different from safety – it is folded back in to the safety process, so worse safety or threat condition is accounted, and maybe that needs to be made clearer
    f. Michel – He can agree to a lot of the opinions expressed in the paper, but the document needs to be adapted to lots of different companies and processes, and this is difficult to put into the document, and we can only put the security inputs in as part of the process interface

g. Chuck – if you are making the change on one side of the interface you have to reflect this on the other side of the process interface. We are developing the same systems, we allocate safety credit to security and so things are going to be mixed. He is struggling to see if there is a fundamental disconnect between the two. Safety is not narrower than security
h. Claudio – We were experiencing a lot of problems with the safety groups as there was a lot of resistance from the safety groups, plus if you drew every feedback line the diagram would not be readable. If you look at the appendix it does say about updating the hazard, so whilst the diagram may not show the link the Appendix does
i. Michel – Also referenced the issues with working group 63 and 18, and believes this is something for the future
j. Romuald – Wants a pragmatic solution, do we need to feedback everything -no because we have already certified aircraft
k. Security takes into account safety outcomes, but there is no feedback unless there is an architecture change you have to reassess the architecture
l. Michel – Security Risk Assessments were communicated with the safety group
m. Varun – Take a snap shot, analyse the vulnerabilities. Security is unique for them as the implementation does not affect the safety
n. Romuald – security requirements become part of the overall system requirements like any design so linked,
o. John – Doesn't see the same level of isolation between the two camps, been a lot of issues in feeding software requirements back to safety, but it is now agreed that derived requirements were seen to sufficient
p. Chuck – People understand the point and a proposed change was made, this may be helpful if appended to the dissenting paper
q. Dave P – difficulties in SAL. 356A are a lot of objectives that are additional to safety
r. Papers to be loaded onto the RTCA site for review

9. Review of the spreadsheet - Michel
    a. Keep in mind it a document we can leave with
    b. Nine comments still in work – which are mainly aligned with the two dissenting g papers
    c. 897
        i. No dissenting opinion, but if the Panasonic dissenting opinion is addressed it should cover this area potentially as well.
        ii. If we don't agree with the dissenting opinion – what is the solution, it is around different DAL and SAL. If we get to Wednesday and no agreement, then Dave will provide text
        iii. Michel showed the changes in the architecture text
        iv. Dave – It does not talk about Design Assurance Levels
        v. Michel – Is this a chapter 5 or chapter 4 change?
    d. Most comments that have not yet been accepted – do have a proposal
    e. Philippe – how do you manage linked comments – Michel - they still require agreement by the group
    f. Linked comments – closed
    g. High comments reviewed that had a proposal

i. 292 – Assets – ‘system’ was used to propose to resolve the comment – needs agreement from Cyrille. Stefan – there is redundancy here with chapter 2 and possible contradictions. New proposal to be made
ii. 487 – closed
iii. 894 – closed
iv. 935 – SAL and DAL – new proposal has been made. Aren’t all security measures aircraft functions – no you could have procedures. Stefan - We have already changed document scope so do we need this. Yes, but if this satisfies the comment – does that matter. Stefan – we do keep repeating things in different ways. Romuald – if it is covered in scope not required. Michel – could be in 1.2. Philippe – this is written negatively. Stefan make a positive statement for 13xx and this is not for 1309. Michel – we have nobody in EASA at the moment. Dave P – the point is that it does not handle safety aspects, which is in line with Chucks DO. PM does not agree that it is an independent process. If you can address it in scope fine. Propose – remove the second sentence and refer to future document 13xx in scope Romuald would like it simplified. Michel – disagrees you don’t close document buy just removing text. Simplified and closed, and 13xx included in the scope. If we get the 13xx actual number, we replace if the number is produced before document is published
v. 1094 – Accepted – explanation was included

h. Medium
i. Medium comments review and closed following notes only highlight any discussion points raised, comments not recorded were closed
ii. 353 – SAL 0 applied to assets that are not security measures
iii. 873 – concern was high design assurance could be high or high SAL, Romuald – why are we talking about DAL. PM – difficult to follow the changes. Stefan will check and should be okay – should be DAL or say design and development assurance.
iv. 899 and 901 – still open waiting on feedback
v. 910 – Use of independence and isolation raised - Stefan – reference 3-5-1 – added. PM – has concerns on what is written –

10. Adjourn for Lunch
i. 910 continued – waiting on GE feedback
ii. 1241- Stefan - Where else do we have objectives applied to standards. Stefan – we are light on the standards then. Michel – doesn’t prevent you to using standards. Michel proposes to close the comment does Dassault agree= closed

b. Stefan - General request – all proposals should have been sent out, Michel – should now use the comment sheet. Stefan. Dave P – send out the comment sheet to the full distribution list to ask them to look at the proposals

11. Security Assurance committee (2 NC, 5 H)
a. 377 – linked to 375 and 376, also liked to the dissenting opinion
i. Chuck if the basic discussion can be resolved, should clear them all. There was a proposal on objectives and the wording of the tables which was fine but did not solve the basic issues

ii. Romuald – need to propose a resolution, and should not be linked to a dissenting opinion
iii. Michel - One solution was worked out for both NC by the sub-group, chapter 4 text has been changed, this is the last chance to get some agreement during this week, and there is time Wednesday and Thursday

b. 848 – Need feedback from Dave P on this – some progress has been made on this and this is linked to Chucks dissenting paper, but can be closed
c. High Comments
    i. 331 - No apparent solution. The proposal is to stop the discussion and close the comment. No time to define new objectives here, commenter notes that tool qualification will not be required for SAL3 security measures on DAL E – comment closed
    ii. 335 – Clarify objectives when independence is required - no agreement has been reached with sub group proposal. The proposal is not to change anything – they don't see how they can clarify independence. Stefan - we don't want requirements for expertise, that will be discouraged EASA. Is it clear when objectives are required for independence. PM – sometimes we want different people. Michel refers back to the definition. Discussion then around testing. PM Independence required for refutation testing. Stefan – organisation requirements – we don't want to make that a certification requirement. Stefan – Are notes associated with the objectives. Stefan – that's how the other standards handle it – so he is happy. WG agrees with the subgroup resolution – if no other proposal – close the comment. Gilles – look at independence again
    iii. 354 and 355 commenters and the subgroup agree – so proposed to close – closed
    iv. 1265 – Resolution proposal was agreed with Dassault, but it is not in the spreadsheet. Proposal is to change the wording in A1.22 – change to Validation that security measures are effective to mitigate risks identified in the ASRA/SSRA - some discussion on the use of validation and verification which is not consistent in standards. John A – are you proposing test here. Michel – the context is important here. PM believes the comment was at item level. Michel – can we agree to close the comment with the new resolution – closed
        1. PM 1217 – back to item level discussion, and discussions on verification and validation. Does something now need to be changed in this document? Discussion ensued around validation and verification. Patrick M is John advising don't use the word effective. Michel - we use effectiveness in the security risk assessment. Change effective to sufficient. Back to effective and back to the subgroup - closed
    v. 334 was closed and commenter disagrees, COTS are SAL 2. Agree to remove the CC2. Verification results discussion starts again. Which refers to comment 1231 – which had been accepted – looks like editorial got mixed up, corrected at the meeting – closed

vi. 340 was closed and commenter disagrees – problem with verification objectives no specific objective for functional coverage. Subgroup says that functional coverage is covered by O6-1 and O6-5 – so no resolution

12. Break
    a. High
        i. 342, 344 hanged subgroup proposals to remove "in compliance with the verification cases" from the end of each activity.
        ii. 345 – replace test cases - with verification elements - John A questions this
        iii. 304, 346, 356, 365, 489, 951, 952, 1155,1230, 1270, 1271, 1277 – closed
    b. Medium
        i. 20,21 – closed 22,23
        ii. It is not intended to be a consensus standard - soften the language and keep the reference. Stefan – we can write document and regulators can change, Varun wants document that is correct and doesn't want to pick and choose. Headquarters want to be harmonised with very few exclusions. Mitch just wants the references softened.
        iii. Resolutions accepted, and comments closed
13. Risk Assessment committee (1 NC, 4 H) – Phillippe M
    a. 445 – Risk consistency check – closed
    b. 1303 – P Marquis – no concerns but if removed there is no help. Closed
    c. 840 – is now a proposal as accepted by Stefan, and comment is closed
    d. 443 - resolution accepted and closed
    e. 456 and 458 – resolutions accepted and closed
    f. Medium and Low – accepted
        i. 175, 176, 177 - closed
        ii. 220 – If we are demanding security expertise – what is required, so disagrees with change – remove the word 'demand.' – agreed and comment closed
        iii. 234 – resolved by previous change
        iv. 836, 843 – closed resolution accepted
    g. Medium and Low Proposals
        i. 201, 280, 281
        ii. 413 - some considerations around the word quantitative – resolution agreed and closed. Stefan recommends it is checked with EASA. Security is evolving, and methods will change with time and methods may need to be adapted and renegotiated with authorities. Romuald – 'statement' not a principal – statement could be misleading.
        iii. 415, 416– resolution accepted and closed
        iv. 446, 447, 448 - introduction of design and environment changes. Changes need to address the comments. Romuald inconsistencies now between the sections. Change the title was proposed
14. ADJOURN
    a. Dave closed the meeting

## 3 Tuesday, April 10, 2018

New attendees:

- Siobvan Nyikos (Boeing)
- Daniel Nguyen (Boeing)

1. Administrative Remarks
    a. Opening remarks Dave reminded everyone that we should not introduce new comments
2. Objectives committee Dave P
    a. 375 and 376 Proposal is not agreed by the commenter and is part of the dissenting opinion
    b. 462 - Claudio asked about keeping track of concerns since we cannot introduce new comments at this time
    c. Dave - Any RTCA document has a comment sheet at the end of the document that you can formally submit to RTCA at any time, and the committee addresses it when they come back together. Dave also offered to to track concerns until publication comes out
    d. Michel - 203, we put down problem statements, topics that need to be worked, we don't know when a new revision will be started (if at all)
    e. Avoid making statements about rule process, may not belong in this document
    f. Claudio will try to form a statement to go into this document and then resolve the issue later
    g. Found at least 3 parts of document that talks about security functions, should be security measures
    **h. Action – replace instances of security function with security measure**
    *i. Going through remaining objectives comments and proposals (see uploaded spreadsheet for complete status and accepted proposals), same for all subcommittees*
    j. Changed functions to measures in objectives
    k. Varun – different process for navigation data, let that be, not the business of this group
    l. John – add a statement that navigation data is out of scope
    m. Michel – there are other databases
    n. Patrick – intention is path forward, infrastructure change to get there, ARAC recommendation, say "as negotiated with authorities" as a path forward
    o. Michel - We define field loadable software, airborne software that fits this, propose to keep airborne software and clarify what this includes to better match scope of document
    p. Varun – microprocessor has firmware you can't access, there is other firmware you can access
    q. Going back to definitions
    r. Varun – don't think you should be getting into data part, already schemes to manage
    s. Patrick - Are we implying that integrity and authenticity should be continuously checked? Or just part of the software load process? Reading objective and what it implies
    t. Phil – lifecycle protection is beyond scope of this document
    u. Michel - GE comment, what does GE say?
    v. Stefan - If we want to use airborne software, then in bold print make it clear that we have definition, people read documents but not definition first, and people will read airborne software and think only software and not that it includes firmware

w. Varun – can't define everything for everyone, need to make assumptions of the reader
x. Close comment, moving on
y. Action to Stefan to reword objective, question is how much should security be included in other standards?
z. Martin – no ARAC standards active today
aa. Varun – don't have rule yet, EASA will have one in a year, FAA four year, "fighting ghosts"
bb. Revise downstream if needed
cc. Martin – I thought charter was to align with ARAC report, currently special conditions and ARAC report have disconnects
dd. Align with what the new rules are / will be
ee. Michel – hear agreement, close comment
ff. Vulnerabilities are treated according to their evaluation objective
gg. Martin – OK with phrasing, what if there is no threat path
hh. Minor threat condition, but no access, maybe it is acceptable to do nothing
ii. Martin – change from "high level" to "refutation" test plans are available, Cyril agrees

3. Document Scope committee (1 H) – Stefan S
    a. Peter - Look at ARP flow diagram, flow to software and hardware, if you have to do network security risk assessment, it includes hardware and software components
    b. Martin – include a statement that all security aspects will consider hardware and software
    c. Varun – when you do assessment, don't you look at entire airplane?
    d. Martin – you do, but you scope based on interfaces
    e. Phil - I don't like modifying our definitions of software and hardware, number of objectives that say software and hardware, sound redundant
    f. Stefan – don't do much for hardware, but then airborne software include hardware
    g. Michel – firmware, not hardware
    h. Dave – running out of time, might need to skip this
    i. Martin – 2.2.2 analysing potential impacts
4. Example Methods committee (2 H, 12 M, 11 L) – Claudio de C
    a. 1011 – agreed and closed
    b. 505 – example methods text – closed with a minor change "airworthiness authority"
    c. 992 – should use the same architecture examples, idea is accepted but time precludes the change – closed
    d. 996 – not possible to implement – Stefan raises comment – why was it not possible to implement – Here is an example but its incomplete. Who will work on and provide the proposal – no volunteers – closed
    e. 1006 – won't be done for the same reason, discussion on why no proposal close and go ahead
    f. 1064, 1066, 1073, 1069, 1071, 495, 632, 634, 1074, 635
5. Certification committee (20 M, 6 L) – Stefan S
    a. All the airbus comments had been accepted
    b. 792 – proposal has been sent out, text was inserted in document and Stefan gave an overview of the proposal.
    c. Wording is aligned with 178 and 254 and adjusted for security.
    d. Romuald, have you checked overlap and inconsistencies to 2-8-1.

e. Stefan proposal for the section is more in line with 178 and 254.
f. Michel – what is the concern and what are we trying to resolve.
g. Stefan – This is making the section more aligned with 'existing' practices
h. Peter Why are these topics in this document, already have guidance and circulars in this area. This should be limited to security specific.
i. Stefan – This is security specific.
j. Dave – does the group understand what is being done with this text.
k. Michel – common criteria missing
l. Stefan – it is still in there. Michel want the change not to go ahead.
m. Need to make text available for review, think about it and vote whether to include

6. LUNCH
    a. During lunch, Peter Skaves uploaded an Electronic Component Management Plan (ECMP) example outline of which the FAA and EASA are publishing A(M)C 20-152 which includes regulatory oversight of this document
    b. Continuation of certification comments 792
    c. Peter concerned that Stefan's new wording will lead to duplicate text, discussed how document is already too long has a lot of duplicate text
    d. Dave – would like opinions of Romuald and Philippe on Stefan's proposal uploaded during lunch
    e. Philippe needs more time with comment, move on
    **f. Action to review and vote on the text**
    g. 1042, 811 closed
7. Back to example method
    a. Siobvan confirmed that the table in appendix F had been corrected, had a similar Boeing comment, close NC from Laurent
    b. 1063, 255 – closed
8. Assets committee (1 M, 3 L) – Phil W
    a. 10 comments – not seen any agreement with the commenter
    b. Phil confirmed process check – silence is acceptance if you notified the commenter and they don't get back to you
    c. 620 – keep resolution of 496 closed
    d. 753 – propose to keep it as it is as section talks about systems
    e. 1299 - closed
    f. Dave Pierce – do not wordsmith the ARAC report
    g. 395,387 closed
    h. 388 – figure proposed – but sub group did not believe it made things clearer closed
    i. 389 closed
    j. 390 – proposed significant changes from ARAC – so closed
    k. 758 – do not believe the comment provides clarified text, so the proposal is to reject.
    l. 207 – linked to 384 which already clarifies text and closed
    m. 297 – closed
9. Trustworthiness committee (2 M, 2 L) – Dan J
    a. 776 – Stefan was happy with the proposal from Dan, but also there was a proposal from Romuald and disagreement in the subgroup.
    b. Dan has provided additional examples – include or not.
    c. Stefan disagrees with intrinsic risk associated with trust.

d. Discussion around trust and the risk assessment process. Chuck raised the previous work that tried to grade trust, but no appetite to grade, so if its good enough to satisfy the need, its binary. Need a new proposal around the first line and intrinsic trust. First two sentences deleted. Closed
e. Comment to put all of it in 2.6
f. Dave – not in favour in disturbing ARAC material
g. Stefan – section 2 explains regulations, 3 explains compliance, don't move wording
h. Michel – reject comment, Claudio agrees
i. Stefan – "inappropriate use" doesn't matter or help here, same with "non-aviation"
j. Be careful of internal vs. external
k. Dave – don't change intent, ARAC direction flows down, not up
l. Stefan – not changing direction, need explanation where external actually means external to the aircraft, people reading this will not be reading this side-by-side with ARAC report
m. Romuald – need to spend time on more critical topics
n. John – talking about services, not activities, don't add words, don't pertain to bullet
o. You can say later that you trust an airline
p. Closed, rejected
q. Stefan thinks there will be impact to applicant
r. Varun – this is not set in stone, can change on next go around if there are complaints

10. BREAK
11. Risk Acceptability committee (1 L) – Phillippe M
    a. Boeing comment on table 2-3, added note after clarifying that risk acceptability table pertains to target system, not access point, comment closed
    b. While Michel logging back in, discussion on dissenting opinions and process
    c. Dave – tomorrow (Wednesday) morning we will discuss dissenting opinions again, please bring comments and views to discussion
    d. Can technically publish with dissenting opinions, however that hasn't been done before
    e. Would push PMC to recognized published dissention opinion
    f. EUROCAE has different processes from RTCA
    g. Stefan – What about accepted means of compliance (AMC)? Does dissenting opinion get to do things differently?
    h. Michel – need EASA in meeting to answer for their end
    i. To FAA, it will look like we punted the issue, and then they write their AMC to match
    j. Looking at impact criteria
    k. Do we want to include no safety effect?
12. Document Consistency committee
    a. Comment on possible missing topics
    b. Stefan – in Paris, we decided to add text as to what is guidance material, where is that material?
    c. Merge text into bullet points under how to use this document
    d. Editing in real time, and
13. Security Scope committee – Phil W
    a. 2 comments left 798 and 1047

b. STPA sec used to define security scope, Stefan would have shortened it, but proposed solution OK
c. Title changed for second comment
d. Comments closed

14. Architecture committee – Siobvan N
    a. Several comments on 5.6.2 and one proposed rewording to address all
    b. Romuald had issue with 5.6.2 integrity of connected equipment principle, is it truly a security architecture principle?
    **c. Action to Siobvan – add clarification wording at beginning of chapter 5, what we mean by chapter 5 considerations (sent before meeting adjourn, will review tomorrow)** – overcome by events, Romuald found the appropriate wording already in chapter 5
    d. For example, whether or not something is implemented off the aircraft or procedurally, it is still a security architecture consideration. If something is not implemented, you need to incorporate it into your aircraft security architecture. If it is implemented off aircraft or procedurally, you are covered.
    **e. Action to Michel – make the following edit since people don't like "…should have some way…"**
    f. The production, maintenance organization, and operator should have a means to check the integrity of the Loadable Software Airplane Part (LSAP) or data loadable equipment prior to dataload.
    g. Went through rest of comments, added rewording as needed
    h. Philippe – lacking a principle on fail secure
    i. Siobvan – discussion in 5.9.4
    j. Michel – that was the new principle added, 5.6.6 Principle 6 Detection and Restoration
    k. Addresses Philippe's concern
15. External References committee – Michel M
    a. 544, 795, 1163 – Closed
16. Level of Threat committee – Adrian W
    a. All comments resolved and accepted except 168,
17. Terms and Definitions committee – John A
    a. Discussed CIA – closed and agreed that these are most commonly used security attributes
    b. Discussed SECSE – New term for SECSE – safety effect caused by IUEI
    c. Independence, diversity, and isolation defined in 3.5
    d. John – don't have term for exhaustive testing, we think of it as alternative method to DO-178C
    e. Varun – what does it have to do with security?
    f. Dave – you try every single input at your interface to guarantee you don't have vulnerabilities, there are alternatives to that
    g. Closing comment on refutation
    h. Michel – internal vs. external can pertain to many things, shouldn't define in document
    i. Stefan – think special conditions, otherwise misleading
    j. Dave – you can't tell the context? Don't assume an amateur is reading this document
    k. Example earlier today in chapter 2
    l. Proposal to replace sub-item with component

m. See spreadsheet for rest of terms & definitions decisions

18. ADJOURN

## 4 Wednesday, April 11, 2018

1. Dave opened the meeting, the morning will involve comment update status, the two dissenting opinions and an outstanding NC
2. Comment status update was given by Michel
3. Discussion on Consensus exercise
    - Still a NC from Claudio in addition to the dissenting opinions
    - Will run through accepted comments quickly to allow time for others
    - Friday is when we will decide if we are ready to publish
    - Dave went over dissenting opinion process
    - Dissenting opinion has these elements:
        - View of issue
        - Rationale for not joining consensus
        - Group that hold dissenting view
        - Consensus group should be headed by chair
        - Consensus group needs to answer with their own paper, needs to be done before PMC (next PMC scheduled for June)
    - Clive via chat – supposed to provide dissenting opinion paper 30 days before plenary
    - Dave allowed exception since these were known issues
    - Sent this exception only to those who provided NC comments
    - Karan is aware of exception
    - Dave plans to have a draft a week from Friday that a consensus group can work to
    - Rebecca (RTCA) provided clarification – individuals don't dissent, organizations do
    - Go through organization's legal process
    - An individual setting up a consulting company can still technically dissent
    - Also, you're either with the dissenting opinion or you're with the consensus
    - EUROCAE process vs. RTCA process:
    - EUROCAE Council approval is process approval
    - RTCA PMC will make technical corrections if needed
    - Anna will join later to provide clarification from EUROCAE side, 10am
    - Consensus exercise Friday morning at 11am
    - Michel – consensus group should be everyone on committees who are not on the dissenting opinion papers
    - Philippe – when can we start draft consensus paper?
    - Dave – might not be needed, wasn't planning to start unless it comes to that on Friday, but members are welcomed to start it at anytime
    - Romuald - Feedback from PMC on how they decide?
    - Dave - Unsure of all possible outcomes
    - Friday will be show of hands, yay or nay publication of document
    - Editor and small group will proofread for editorial comments only
    - Possible to get approval to publish with dissenting opinions
    - Not entertaining new comments, opinions, etc.

- Stefan's questions from chat:
    - Do authors of dissenting opinions need to attend PMC? - for EUROCAE TAC, organisational representative needs to present their Dissenting Opinion
    - How does FAA/EASA react to dissenting opinions when raising AMC?
- Martin (echoing Stefan's concern) – in process of next few days of working on DO, what if someone who previously did not have a NC now has a NC?
- Don't make a change that leads to another conformance
- Dave – if we make a change to a low comment that leads to a high comment (or NC), we won't make that change
- Still a consensus, look to committee
- One vote per company

4. Dissenting Opinion One – Panasonic
    - Varun – clarification, you can put security measures on DAL E systems, but you can't take credit for them
    - Philippe - DAL E is for safety, afterwards if high level security measures implemented, we can provide security evidence, commensurate to risk
    - Martin – if you as a regulatory are not going to accept SAL, we have a bigger problem. Not only about allowing secure measure on DAL E system. DAL for safety, SAL different
    - Varun – not going to change 50 years of precedence
    - Martin – if we apply to SAL to entire system what is difference for segregation process? Can do SAL on entire system or partition
    - ARAC said you don't have to do security on minor system, so you did change precedence, just the other way
    - Varun – DAL E don't have to meet intended function
    - If you put security in DAL E system, need to partition it and handle it separately
    - Don't connect it to network
    - Dave – SAL credit but not DAL credit
    - Martin – DAL E with security controls and credits already done, passed through regulators, this proposal is technically a change to what's been done, making it more difficult to meet special conditions, make it more costly and not getting anything better than what you get today
    - *If we go beyond this, will result in Boeing DO*
    - Dave asked Martin to restate problem:
    - *Martin - Problem is today we take credit for nonessential systems, we need security measures for end to end security solution, if we can't take credit for this on DAL E system, puts hold in end to end security, makes it more difficult to meet special conditions*
    - *Steve – my problem is intended function; your security control has intended function and you need to protect it from other side*
    - Philippe – focus on Sal evidence, not DAL evidence
    - Michel – document talking about security measures, other ways to implement security measures, can apply SAL to DAL E equipment, give evidence that it protects, minimum DAL that is proposed will restrict SAL so much that we can't put it in document
    - Chuck – everyone assumes existing system, add architectural feature with security, leave safety assessment untouched
    - Patrick - Can you imbed DAL D function in DAL E LRU?

- Phil - With caveats
- Steve - No, safety assessment then determines hazard for system is minor
- Patrick - Building on concept, as time goes on, systems will be more integrated, may need to assign different DAL to different components in box
- Intent of this document is to create foundation for raising DAL of *component*
- Look at objectives in this document, raise DAL of security measure
- If a system is dependent on a measure, needs appropriate SAL
- Chuck – already standards for isolation, higher assurance isn't necessarily higher DAL, this committee is moving in opposition of industry in terms of how hazards are assessed
- Trying to understand, where assignment of SAL to a DAL E or DAL E portion of a system, how is that different from assigning to entire system?
- Steve – agree with Chuck, that's my problem with this, no safety effect system now has functions that have to work, don't care about DAL D or higher, only in this instance you feed back to safety
- Industry framed on no safety effect, now something that matters
- Steve OK with SAL process and isolation, take one instance and feed it back
- Stefan – not seeing changes that move DO one way or another, unless someone has actual changes today, let's focus on something else
- A lot of comments to go through
- Dave not going to change agenda
- Michel – agree with Stefan, we are repeating discussion points several times, no movement forward
- Varun restated position and threatened non-approval at PMC
- Mehdi - Putting SAL on DAL E functions would improve security of system
- Romuald – we have precedence and in-service experience, security measures in DAL E systems certified by both FAA and EASA, surprised that we are challenging something that was previously acceptable, think propagation, today we are designing and certification is ongoing, to protect
- Prevent threat from propagated to other aircraft systems
- Varun – that was because they were secondary controls
- Philippe – subject to both evidence, no safety effect equipment is wrong, implements security evidence
- Martin – Varun contradicted his position, special conditions require more than one layer of protection, we are asking for one level of protection at a lower DAL, need to be able to do that
- If you don't accept SAL, that is a bigger concern, why are we talking SAL if you can't take credit?
- Varun disagrees with Martin's second conclusion
- Peter – been using ARP for 50 years, people who want SAL don't understand DAL, as soon as you find failure mode in DAL E system with security controls, no longer DAL E system
- Peter not going to NC because he can make the SAL work if needed
- Claudio – 2 measures against catastrophic effect
- Varun – I said you can put security controls at DAL E
- Claudio – now you're saying you won't approve it, dataloader example, need something in the middle
- Michel – will our document change situation in practice?
- Not something we can solve here

- Mehdi – We did take credit for assurance on DAL E
- Patrick – I have proposed solution, but we can look at Panasonic proposal solutions first
- Martin gave example of change process and feedback from Boeing process
- Looked at Panasonic solution
- Martin good with feedback to safety, we already do that (part 1 of solution)
- Not good with requiring partitioning (part 2)
- Take out and let applicant figure that part out?
- Patrick – concern is propagation
- Phil – propagation address in part 2
- Michel – see appendix A, consider threat conditions that may change safety assessment, did not get agreement from committees on making it work in a better way
- Romuald – security is a new external threat to aircraft, need to be innovative on how to address, no need to stick to classical process
- Dave - Does proposal keep you from something you'd like to do?
- John – change to system -> reassess safety effect, might be linked to a more critical box
- Reviewing Panasonic proposal
- Michel – leave security function discussion out for now, has to do with Embraer NC
- New term for SECSE – safety effect caused by IUEI,
- Martin summarized Boeing position for first point, in general we agree, this addition might even address Chuck's DO
- Looking back to 4.2.4 security verification objectives
- Romuald thinks this section fully addresses point 1
- Dave – will the Panasonic proposal (point 1) hurt anyone if added to the document?
- Do Steve and Varun agree with Romuald?
- Made slight edits to proposed wording, reviewing
- "…safety assessment associated with the initial design or change to type design" at end
- Wording approved for solution point 1
- Moving onto point 2
- Siobvan – Boeing rewrite of sentence appended to independent and isolation principle:
- *In the case of security functions implemented in trusted**,** no safety effect systems for the purposes of preventing propagation of threats via those no safety effect systems, independence and isolation of the security function from the no safety effect system functions may be implemented.*
- May vs. should
- Phil – change back to should
- Martin – partitioning is up to applicant
- Varun agrees
- Treating whole system vs. partition
- Dave – again, is text flawed or unacceptable? If it doesn't hurt your position, do your best to accept
- Romuald - In safety, decisions up to applicant, security should be the same way, up to applicant in how to comply with regulations, would prefer to stay with "may" instead of "should"
- Michel – doesn't add useful info to principle, would prefer to add sentence to additional info section of principle rather than principle itself
- Make it a note
- Also, security functions should be replaced by security measures

- Several people wondered why “trusted” was added
- Keep “may”
- Martin - OK with taking out “trusted”, was trying to distinguish the IFE

5. Dissenting Process – Anna/Rebecca
    - Michel – RTCA and EUROCAE have same process, with exception of dissenting, that’s a little different
    - Stefan question from chat - How do we ensure that PMC and TAC come to same conclusion?
    - Anna – consensus group provides position as to why comment cannot be resolved, presented by working group or subgroup chair
    - Dissenter presents whitepaper explaining why doc or section is not considered acceptable, resolution of comment, why discussion in working group not satisfactory
    - Required to state every effort has been made
    - Rebecca – works that way at RTCA
    - Stefan - Would dissenters present to TAC? Or only PMC?
    - Anna – join document, if dissent comes from US, needs to be presented to both PMC and council (TAC)
    - How to get PMC and TAC to agree? Coordination needed
    - PMC June 21, need document by May 10
    - Rebecca – turned over to secretariat, RTCA and EUROCAE
    - Technical questions will go to technical experts
    - This time council gets it first, then PMC
    - Anna – might need special coordination
    - After that, meetings scheduled for October
    - Reason for dissenter being org and not a person – don’t want one person from a company to dissent and another person from same company to be in consensus
    - Three pieces
    - Document
    - Dissent
    - Rebuttal
    - PMC is reticent to publish document with dissent, go back and try again
    - Regulatory thoughts
    - Varun – need to address everything this week, won’t go away
    - Cyrille – are there any documents in EUROCAE with dissenting opinion, only happened once before and that was solved in the last minute
    - Dave – It’s a situation we don’t want to be in, so let us try and resolve this
    - Thanks to RTCA and EUROCAE for their support in these documents

6. Dissenting Proposal - continuation
    - Agreement of point 2
    - Point 3
        - Section 3-5-1 suggest look at the measures and see if it addresses point 3
        - Review of the modified section with Panasonic mark-ups
7. Measures
        - Dave – context of isolation – what is the point of it?
        - Faults may or may not cause different assurance levels

- Phil – introductory text, OK with removing, need to further down

8. Lunch
9. Measures
    - Continuation of security measures to include Panasonic proposed wording (point 3)
    - Phil - Don’t want to depend on something of lower assurance level, but if you want to call it isolation, I’m OK with that
    - Cyril M. - Intent of doc was to put SAL on security measure only, sentence seems to emphasize there is a case of environment without security assurance
    - Put application into partition and measure into another partition, embed security measure
    - Phil - should have same assurance as security measure
    - Cyril - Developed in existing partition with safety assurance
    - Phil – if you are making that assumption, then I agree
    - Agreement, just need right words
    - Dave – need to remedy “flawed text”
    - Cyril - Text is constraining, need to differentiate between security measures and environment
    - Martin – don’t want to constrain or tell you the design space, when you look at common mode sections and principles, then you get to right solution, adding text here doesn’t prevent right solution, however it constrains solution, which is why I suggested rewording
    - “May need to be” instead of “needs to be”
    - Michel - Originally, independence meant if one fails, the other won’t automatically fail
    - One is not dependent on the other
    - Statement belongs in isolation and not independence
    - Can live with statement in both
    - Martin agrees, if it closes dissenting opinion, do it
    - Close to closing Panasonic NC and DO, looking at recommended text, “If the authentication service is of lower assurance…”
    - Martin - Something that prevents unauthorized access, then have something that restricts that access at certain ports, protocols, and IP addresses, then two have to work together, two are not independent for the overall security effect you’re trying to get
    - Combined effectiveness rather than assurance
    - SAL is used to augment, not forcing anyone to use SAL
    - Add bullet to Isolation part
    - “A security measure that run with or on a lower assurance operating environment…”
    - Phil – trying to draw example where other item is not a security measure
    - Michel - No effectiveness could be due to missing assurance
    - In Safety, lack of independence does not mean you have lower DAL
    - From Stefan Schwindt (chat):
    - It just means you don't have two separate measures

- For security, it should be the same - you have achieved all of the security objectives - i.e. assurance - but it won't be effective
- Is the change now agreeable
- When the draft document is complete and the DO points are present the DO paper will be withdrawn after they have seen complete draft with the changes
- NV Comment 613 and 897 closed
- As long as we keep the edits, Panasonic is withdrawing the DO

10. Second dissenting Paper from Chuck
    - Chuck summarizing DO
    - The issue here is dissociation of vulnerabilities/errors and SAL/DAL
    - Foundational Issue is that safety and security must come to the same conclusions
    - Martin – still feedback to safety
    - I do not see that we have to be constrained by 326A process flow, issue is safety is the primary question
    - Chuck - No exception to safety process, safety finding is a safety finding, safety experts need to find consistently, correct understanding is whatever capability, can't predict how it will fail, failure due to IUEI is one way to cause failure, not only way
    - Problem is two organizations interpret two different way re: safety assessment
    - Stefan – don't see where in document we would have different severity for same effect
    - Can put in wording saying two sides (safety and security) need to talk to each other, but that's an internal process within the different companies
    - Sam - Effect already identified in FHA, in aircraft and down to systems
    - Michel – every IUEI needs to be handled, but not just one safety process, people doing an FHA are used to dealing with safety excluding malicious attempt, now we add safety looking specifically at malicious intent, important to come together
    - Varun – want to take care of low hanging fruit, last bullet regarding "possible to conduct safety assessments" addressed in previous DO discussion
    - John – hazard is not the event, safety people ignored potential hazards in air gaps in the past, need appropriate safety analysis along with security doing their analysis
    - Martin – in principle I agree with Chuck, but I thought it was covered in DO-326A appendix stating that you would flow back to safety process, from security perspective, we came up with common mode failure not considered by safety because it's intentional
    - Steve – can I do something you already accounted for in FHA that changes result? More frequency? Something you didn't account for? If yes, then you need to feedback to safety
    - Having said that, do we do this in this document?
    - Philippe – functional perspective, FHA as it is, what would happen is impact assumptions
    - Varun – those requirements are intended function
    - Romuald – safety assessment accepted by authorities, don't see why new document in industry should conflict with what is already accepted
    - Dave – general agreement that security findings that impact safety should be fed back to safety

- If we are in general agreement, now what?
- Chuck – concern is that there is an understanding that document does not require safety assessment to account for IUEI
- Dave – what is the issue? How safety and security come together? How much?
- Varun – if event, box doesn't care where event came from, either way there is a failure in the chain
- Patrick – is there a proposed resolution we can view?
- Chuck sent a proposed redline to Chapter 4 security assurance
- Philippe – DAL is under frame of safety, now we are in frame of safety + security and DAL doesn't address that
- Chuck – SAL doesn't address all requirements of development assurance, two different processes, both are pointing at each other saying not adequate
- Reviewing wording
- Sam – remove "risk", just say safety assessment and security assessment

11. Adjourn – team dinner

## 5 Thursday, April 12, 2018

1. Administration
    - Michel provided comment status
    - Michel proposed to go through comments by priority.
    - Waiting on more people to show up to start the discussions on the NC
    - Still waiting on an NC from Claudio
2. Starting with the high comments
    - Stefan – proposed new verbiage for comment#1027 added a noted in Section 3.1 to define the term "airborne software"
    - Stefan – sent a list to Michel of a list of his comments that are ready to be reviewed
    - Phil – Concerned about the definition of AEH and it should include hardware components
    - Comment 203 – Concerned with the truth of the statement with the release of SPECTRE and MELTDOWN
    - Stefan – Need to get applicant to understand of the partitioning scheme is adequate. There needs to be analysis of, if the target needs confidentiality or not.
    - Michel – Concerned already in addressed in Appendix I.2 (Notes Column)
    - Comment 435 -
    - Stefan – Check in proposal to validate that the Chapter 5.1.4 got updated in section 3.5.1. If it has been updated multiple linked comments to it can also be closed
    - Comment 865 – O8.6 – Include high level refutation test plans are available
    - Patricia Fuilla – On Phone – Sent email to Michel with updated text okay to close if text "High Level" is removed in text "High Level Refutation"
    - Comment 292 –
    - Claudio – Sent Michel a proposal yesterday for comment 292
    - Stefan in chat - Michel: table for Common Mode Proposal has all changes proposed included - all good
    - John Angermayer in chat - test plan has no CC category. Also, there is nothing about what is in it.
    - Stefan in chat - John - is this related to the last comment we discussed?
    - Michel – Wait for Cyril to show up to close this comment
    - Comment 335 –
    - Armelle – Has new proposal for, do we need to replace "independence" for

verification/validation from the people who performed the output

- Stefan – add an additional note to remind what independence is
- Varun – Understand what you're saying but why do we need to spoon feed the document to people, they should know what independence means
- Stefan – just trying to make the commenter happy
- Michel – Does not want to add so much detail to appendix unless preferred
- Dave – Agreed
- Varun – Agreed
- Dave – Unless we get strong support for adding in the detail, we probably will not add it.
- Stefan – In the sections necessary just add a reminder of independence and point to glossary
- Varun – Where do you stop putting reminders?
- Varun – Do you think its value added if not don't put it in, we need to reduce the size of the documents not increase it
- Patricia Fuilla (on phone) – would like to discuss offline with (PW?) to provide a small updated not for consideration
- Dave – Chuck's got to leave in 40 minutes would like to discuss Chuck's DO
- Michel – Added Chuck's proposal in text
- Ravi In chat - Hi all based on what was discussed yesterday is the use of SAL mandatory
- Martin in chat - The use of SAL is not mandatory, but you will have to augment DAL with the missing security requirements/testing

3. Dissenting Paper - Chuck
    - Dave – Review paragraph 3 for updates and see if it's acceptable
    - Michel – Not sure the value of this paragraph
    - Dave – Inserting a vulnerability is always an error (including the ones you didn't consider)
    - Sam – Strike erroneously out
    - Mitch – The goal of the process is to ensure the final product is acceptably free of exploitable vulnerabilities. Don't think the phrase captures this in totality
    - Chuck – If you go to section 3 identifies 2 types of vulnerabilities (implementation, types that are inherent in the design) the reason for this is to say we know about our known vulnerabilities, the point of security assurance is to eliminate errors that are created with the product during development. Don't have any big objections from removing erroneously.
    - Gilles – Supplier is part of the trusted development (should be included)
    - Varun – It's not a trusted thing, trusted is the malicious error
    - Michel – The statement is misleading propose we remove this word
    - Chuck – you won't leave a known vulnerability in
    - Philippe – may want to leave vulnerability if acceptable
    - Chuck – if we are starting with the premise that we are leaving things in intentionally that's not the point of the process. Leave in a word that suggest that we will leave in known exploitable vulnerability is strange. Looking for the product to be free of exploitable vulnerabilities.
    - Michel – Final product is acceptably free of exploitable vulnerabilities
    - Philippe – Agree with Michel, system may have vulnerabilities that are known, this is not correct for the unknown vulnerability
    - Martin on phone – remove the terms known and unacceptable make it higher level and let the applicant determine what acceptable is. Taking term out makes its less exclusive.
    - Varun – Agree with martin
    - Chuck – You do know what vulnerabilities you don't know about. If you go through this exercise it is unlikely you don't know about any
    - Discussion of acceptable vulnerabilities that are not fixed yet as well as unknown vulnerabilities
    - Mitch - Open PRs on systems in service
    - Stefan on chat - Look at number of Open PRs on existing aircraft

- Michel – Proposal? Final product is acceptable free of known and exploitable vulnerabilities, which may be introduced during development
- Chuck - Sentence presumes security assurance has not been done, but it has to be done to discover unknown vulnerabilities
- John - Why would you put something in on purpose?
- Philippe – failure approach and vulnerability approach, developing complex system, impossible even with best process to identify all vulnerabilities
- Chuck – "known" steering sentence in wrong direction, language issue?
- Michel – doesn't change objectives or interpretation of objectives
- Varun – during risk assessment, looking for unknown issues, that's the point
- Dave – to resolve NC, do we need to remove known?
- Chuck – probably don't
- Moving onto last part of Chuck's proposal
- Want to prevent exchanging opinions and actually move toward solution
- Michel - Airbus has problem with Chuck's proposed wording
- Should statements can be interpreted as certification requirements
- Martin has same concerns and has suggested edits
- Making edits to proposal, but Chuck needed to leave
- Dave - If it feedbacks back to overall safety of aircraft, Chuck will be happy, no one expects safety and security to run in a vacuum
- Will revisit edited proposal when Chuck comes back
- Cyrille R. from chat - EASA does not support the fact that the DAL is driven by the security threat condition. We are looking at security properties of the systems some of them can be addressed by the DAL driven by the safety assessment. They may be complemented by additional activities.
- Will clarify comment when Chuck comes back

4. *Discussing Claudio's NC comment*
    - Claudio - Idea here to explain security for safety does not follow cascades, identify needs and security measures, then arrive at requirements
    - Phil - If there is an identified security requirement to protect safety solution, not just business needs
    - Claudio - Idea is to explain we may find security function, it is possible for safety, but usually we define security function due to business or whatever reason
    - Phil - There is no security function to be developed from identified need – actually you can have security for business reasons
    - Martin - Nothing wrong with what is stated, can be stated simpler, security can be developed for both safety and business reasons. Processes developed here are for safety reasons
    - Michel - Security functions can be developed for both safety and business
    - **Claudio good with proposal, everyone approves, close NC comment**
5. Dissenting Paper Continuation
    - Michel – Does document enable you to work within regulatory?
    - People in room want to remove sentence "Because impact severity…"
    - Michel - One interpretation of DAL assignment, may be others, don't want to start debate in this doc
    - Dave to Chuck – will it still maintain your position if we remove sentence
    - Effect of loss vs. cause of loss
    - Finished editing paragraph, got agreement from Chuck, in room, and on phone
    - Dave to Chuck - Expectation is when you see evidence that DO was addressed by changes in the document, you remove DO, same deal as Panasonic
    - Last change to address Chuck's DO
    - Redundant with changes already implemented, Chuck OK with not putting that paragraph after all

- **Chuck agreed to remove DO!**
- No more dissenting opinions or NCs

6. Michel – 12 high comments to get through
    - Looking at security measures comments again
    - Martin – one comment left from Claudio that isn't 100% addressed
    - As before, look at spreadsheet for status and resolutions
    - "Independence may be obtained by qualified tools"
    - Cyrille M. – ambiguous statement
    - Unless developed in house, will be costly to qualify
    - Martin – may statement, up to the applicant
    - Stefan – doesn't mean someone has to do it, applicant decides if it's cheaper to develop or to purchase
    - Martin – need another group to provide independence
    - Varun - Two separate tools from separate vendors, even if not qualified, still have independence
    - Michel – we should reject comment and not add note
    - Martin OK with it since it is a "may" statement and optional
    - Both notes are gone, comment closed
    - John agrees
7. *Lunch break*
8. Process for Friday
    - Tomorrow (Friday) at 11am there will be a consensus exercise and vote
    - Not expecting new dissenting opinions
    - One vote per company
    - Caveats on vote
    - Correction of editorial problems is one condition of vote
    - If we don't resolve rest of comments today and tomorrow morning, we may also have a caveat on those
    - Stefan asked about resolution of independence note
    - Michel confirmed both notes are gone, comment closed
9. Comment Resolution
    - Michel will speed through comments, if someone has an issue with a resolution, stop him for a discussion
10. Example Methods
        - SAL comment addressed, but no word yet on whether or not proposal was accepted by commenter
        - Dave – how do we address such comments?
        - Michel – the comment is M or lower and addressed, so we can still proceed even if the commenter has not acknowledged
        - Question now is whether to incorporate change if we don't hear back, committee can decide tomorrow
11. Logging comments
    - Ed Hahn, pilots' association, comment on 611
    - Last paragraph, talks about conditions under which maintenance actions deferred
    - Varun – you won't know at end of flight if it was caused by security event or not
    - OEM needs to examine logs
    - Ed - If security event known to occur…
    - Varun - Exactly, won't know if event has occurred or not until applicant looks at data log
    - Romuald - Minimize pilot workload due to security, as long as safety isn't compromised
    - Ed - If there is a compromised piece of equipment on aircraft, no way to know until investigation is done, are other systems compromised that are connected
    - Varun – in practice, new box or reload box, not going to ground airplane for weeks of

investigation
- Patrick – attempts and false positives, those are collectively looked at with other system logs to determine if event has occurred
- Take advantage of vulnerabilities that permit behavior
- Most logs provide the basis for system wide analysis
- Isn't a binary scenario that says attack was successful
- Michel showed four square mapping un-occurred, occurred to legitimate, unwanted
- Brian Hoffman on phone, also pilots' association
- Brian – if there is a security event, not going to fly plane until it's fixed
- Maintenance needs to find an airworthy replacement
- Varun – we don't have a message that pops up saying an event occurred
- Only going to have bad dataload message
- Will see system failure but will not know if caused by security until much later
- Chuck – there may be learning that contributes to fault isolation, but that's the closest we have today
- Michel – haven't heard any changes, time up for this discussion, doesn't belong here anyways
- Mitch – if we drop "optional", table may be forced on everyone

12. Threat conditions comments
    - Reviewing diagram 3-3
    - Cyril had comment to match steps/text to diagram
    - Phil – go back to comment about changing security domain
    - Deleted part about lower security assurance
13. COTS comments
14. Document structure comments
15. Current status – 150 comments to go!
    - Under 4.1.4, note about security guidance
    - Siobvan – what is meant by objectives in section 2.4, that section lists certification evidence
    - Not objectives
    - Documents? No because certification evidence can be packaged differently / in different document per applicant decision
    - Just say security guidance is identified in section 2.4…
    - Relevant security guidance listed in PSecAC (since there are 3 different types of certification evidence that fall under "security guidance" listed in 2.4
    - Security assurance comments
    - Validation note under validation definition – validation also used in context of software
    - Is such a note necessary?
    - Keep note, close, move on
    - Stefan – No objectives for supply chain, QA, or process
    - Quality assurance or process assurance will do nothing
    - Varun - Implemented in software itself and that has requirements, so it will be done
    - Stefan - DO-178, not ED-203
    - Varun - Why does it matter?
    - What about auditing?
    - Michel – include auditing of security processes
    - Varun - Augment current checklist for QA and include it
    - Stefan - Fights with suppliers will result
    - Patrick - Developing software to SW guidelines, system guidelines, nothing in this standard says that DO-178 and other standards don't apply
    - They still apply, there are peer reviews
    - Going until 6pm today get through more comments
    - Certification comments

- When making changes to section 2, keep minimal since they came out of ARAC report
- Looking at section and comments on STC
- Allowing for obtaining data package from a third party
- Mitch - OEM not involved, third party does STC. In that case OEM doesn't have data package it is third party. It's whoever does the STC
- Dave – all of that can be figured out by applicant, remove sentence
- Phil – need to run it by Steve
- Stefan – OK whether you delete sentence or leave
- Phil – deleting sentence means deleting ARAC text
- Varun – applicant is free to propose, and they run it by regular
- Mitch – we are in violent agreement with what's on screen now
- Dave – not a shall statement, just need the data
- Particular statement was already argued in ARAC
- Romuald – restate "with the involvement of the OEM, or third party, if necessary"
- Risk assessment comments
- Added appendices reference, but B not included because referring to method appendices
- Some lower level comments are actually editorial
- Objectives comments
- Mitch - Use term "material" instead of objective or section, and it's generic
- 1 high comment proposal for tomorrow
- 20 more low
- 2 hours to get through them tomorrow before vote
- Start time 8:15am tomorrow

16. *Adjourn*

## 6 Friday, April 13, 2018

1. Comment Resolution
    - Different process today – go through "hot topic" comments first
    - For the remaining comments, everyone should review on their own in the room and speak up if they have an issue with a resolution
    - Continuation of comments, see spreadsheet for official status and resolutions
    - Looking at addition to security specific principle, security testing should not introduce new vulnerabilities
    - Phil – sometimes you need to add interfaces to do security testing
    - Stefan - Flight test interfaces remain even after flight test
    - Phil - Keep this principle and address flight test in another principle in another revision?
    - Varun - Hardware interlocks that don't allow using ports when not in flight
    - Martin - Software interlocks too
    - Phil - Put back word security if this is a security specific principle
    - Michel – agreement to keep as is, close comment, and add another principle in a future revision of the document
    - Michel - Accept all the language comments (related to editing)
    - Varun - OK as long as technical content isn't changed
    - Status as of 10:30:
    - All NC, high, medium, and low comments have been reviewed, accepted, and closed!
    -

2. Editorial comments
    - Michel proposes to address and close editorial comments on his own and will let us know if any are not actually editorial
3. Consensus Exercise
    - Consensus exercise – Dave
    - Process steps:
        - Comment disposition
        - Consensus approval
        - Final edits – Dave, Michel, Stefan, and Tim Tinney on editing committee
        - May 8 submission to RTCA and EUROCAE, but needs to be done a few days ahead so organization who submitted DO can view
        - EUROCAE and RTCA PMC meetings both June 21
        - RTCA can get document out 24 hours after PMC meeting
    - Moderated session helped with consensus
    - One vote per company/organization
        - Yes vote – agree to publish doc
        - No vote – don't agree to publish, needs DO, already received and addressed 2 DO
    - RTCA and EUROCAE may need to make slight edits as needed
    - Karan – want to keep integrity of document and truly make it a joint doc
    - Michel – two high comments re: renumbering of assurance objectives
    - Dave gave special thanks
    - Kudos to Michel for his work on the document as editor and keeper of comment spreadsheet!
    - Group picture
    - Joint committee – one raise of hands
    - Yes vote first
    - **Unanimous yes vote in room!**
    - **Unanimous yes vote on the phone/webex!**
    - **Unanimous opinion to publish document!**
- Varun – thanks everybody who has contributed and the tremendous effort that has been put into the working group and this document
- Cyrille – We have the 648 rulemaking task, we have the EASA task who will create an group to allow a quick transition to the new rule and the AMC
- If you have concerns in the document – for next revision send to Dave P or use the change request process
- EUROCAE has approved a new TOR and this is being looked at by FAA and RTCA

4. Meeting is Closed

## 7 Main decisions and actions

| Decision to be made | Decision | Date |
|---|---|---|
| Publication of document | **Unanimous opinion to publish document** | 13th April 2018 |
| | | |
| | | |

/s/
Siobvan Nyikos
Secretary, SC-216

/s/
Clive Goodchild
Secretary, WG-72

CERTIFIED as a true and accurate summary of the meeting