EUR 89-18 / WG72-109
RTCA 107-18/SC216-082 St Denis and Washington, 4 April 2018

Summary of the Meeting of RTCA Special Committee 216 (Meeting #38)
EUROCAE Working Group 72 (Meeting #50)
Aeronautical Systems Security

DATE: Mar 19th to 23rd, 2018

PLACE: EUROCAE Paris
9-23 rue Paul Lafargue
"Le Trangle" building
93200, Saint-Denis, France

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

ATTENDEES:

					March 2018				
Name	**First Name**	**Company**	**SC-216**	**WG-72**	**19**	**20**	**21**	**22**	**23**
Angemayer	John	MITRE	X		T	T	T	T	T
Ayari	Mehdi	Airbus		X	P	P	P	P	
Bates	Steve	Panasonic Avionics Corporation	X		P	P	P	P	P
Call	Martin	Boeing	X		P	P	P	P	P
Descarques	Gilles	Thales		X	P	P	P	P	P
Flores	John	FAA	X			T	T		
Fuilla	Patricia	Apsys for Airbus		X	T	T	T	T	T
Gauthé	Armelle	Apsys for Airbus		X	P	P	P	P	T
Gobbo	Giles	Airbus		X	P	P	P	P	
Goodchild	Clive	BAE Systems		X	P	P	P	P	P
Grant	Chris	UTC	X		T	T		T	
Groote	Anna	EUROCAE			P	P	P		
Haury	Christian	SAFRAN		X	P	P	P	P	
Henrique de Castro	Claudio	Embraer		X	P	P	P	P	P
Hoffman	Brian	ALPA			T	T	T	T	T

Hofmann	Karan	RTCA	X		T				
Hrubesz	Marek	Department of National Defence of Canada	X				T	T	
Jing	Owen	Department of National Defence of Canada	X		T	T	T		
Johnson	Dan	Honeywell	X		P	P	P	P	
Khanna	Varun	FAA	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	P	P	P	P	
Moreaux	Jean-Paul	EASA		X		P	P		
Morrissey	Patrick	Rockwell Collins	X		P	P	P	P	
Nori	Ravi	Teledyne Controls	X		P	P	P	P	
Nyikos	Siobvan Megan	Boeing Commercial Airplanes	X		P	P	P	P	P
Pacher	Martin	European Cockpit Association		X	P	P			
Pierce	Dave	GE	X		P	P	P	P	P
Rosay	Cyrille	EASA		X	T	T	T	T	T
Royalty	Chuck	Aerospace Systems Cyber Security	X		T	T	T		
Salgues	Romauld	Airbus	X		P	P	P		
Sampigethaya	Krishna	UTRC	X		P	P	P	P	
Schwindt	Stefan	GE		X	P	P	P	P	P
Shuang	Zhang	Avic	X						
Skaves	Peter	FAA	X						
Tinney	Tim	AAB			T	T	T	T	T
Trope	Mitchell	Garmin		X	P	P	P	P	P
Verna	Brian	FAA	X		T	T			
Waheed	Mohamed	Aviage Systems	X		T		T		
Waller	Adrian	Thales		X	T				
Watson	Philip	Panasonic Avionics Corporation	X		P	P	P	P	P

P In Person, T telephone

1 Monday, March 19, 2018

1. Welcome and Administrative Statements/Remarks
    - Around the room and phone introductions
    - EUROCAE Remarks by Anna & Christian
    - 1334 comments – shows interest from community in this standard
    - DFO statement from Varun to make it an official plenary
    - Karan reminded everyone of RTCA policy to include no proprietary information
    - Agenda review
2. EASA/FAA Remarks and Regulatory Status – Cyrille R/Varun K
    - Cyrille Rosay (EASA) not on phone yet, Varun going forward with FAA remarks
    - Need harmonized position, otherwise implementation goes haywire
    - Key goal this week
    - We are a consensus party building a consensus document, otherwise we fail
    - Cyrille Rosay joins meeting and reinforces the FAA comments
3. SC216 WG72 Sept Minutes Review and Approval – Siobvan N
    - More important thing that came out of December meeting was voting yes to go to FRAC / OC
    - No objections to minutes from group – minutes approved
4. FRAC/OC Comment Period Overall Status – Michel M/Dave P
    - Dave Pierce gave an overview on the FRAC/OC comment status, received 1334 comments of which 37 are non-concurs and 190 are high comments
    - The FRAC should be considered effective due to the number of comments
    - Some of the M comments are at the same level as H comments and are going to need careful consideration by the editorial groups
    - SAL/Objectives/Assurance – received the most comments
    - The planned meeting in April is scheduled to be the last meeting so the documents need to be completed by the middle of May
5. Rules of Engagement – Dave P / Michel M
    - Statistics
        i. 1334 comments, record?
        ii. 37 non-concurs, record again?
        iii. 190 highs
        iv. 29 companies with multiple commenters
    - Dave reminded everyone next meeting coming up quick, week of April 9 at RTCA in DC
    - Anna - EUROCAE doesn't have a fixed deadline, has approval by correspondence
    - RTCA PMC needs document 45 days prior to meeting
    - June 21st PMC meeting means approval needed early-May with turn over to RTCA NLT May 8th
    - 2-3 weeks to do editing and proofreading of documents, need to be efficient, need volunteers to help with final proofing

- Criteria for the comments – a reminder
    i. Non-concur – Is a blocking comment and should only be put out if technological issues, safety concerns, misleading that makes that part of the document unacceptable – Must be qualified by detailed explanations and resolutions. If committee cannot agree, the RTCA and EUROCAE have a process that will look at the issues and the council and PMC can adjudicate

6. Dave – rules of engagement, look at highs and non-concurs this week, depending on editorial groups to manage, not much time to discuss each one
    - Monday through Wednesday – editorial group presentations
    - Thursday & Friday – time reserved for further discussion needed
    - Topic for later – additional flexibility in document?
    - Opportunity to go into another room and have a smaller side conversation for topics
    - Michel – thank you for contributions to comments and proposed solutions
    - Keep up engagement over next two weeks so we can get document ready
    - D Pierce discussion on the high-level issues, most of the issues are around SAL/Assurance and objectives
        - Main comments
            - Use of SAL should be optional
            - Is a security measure also an asset
            - Goal to maintain ARAC report as closely as possible
            - Objectives – what to do with overlapping, should focus on a strict definition of SAL
        - Need consensus and need to be able to work either methods and not go down a company line
    - Michel – distinguish personal opinions from company positions
    - Regulatory view – what does document provide as potential MOC? Even if it doesn't directly express everything
    - Martin – can we review criteria for different levels of comments? (NC, high, etc.)
    - Anna discussed:
    - NC – blocking comment, tech issue, safety issue
    - Dissenting opinion process – RTCA PMC and EUROCAE tech council review and adjudicate
    - Karan – need to get through NCs so that we don't get into dissenting opinion situation and don't reject document
    - All NCs will be addressed

7. Architecture committee (1 NC, 11 H) – S Nyikos
    - Resolutions have been generated for Non-Concurs and High,
    - Non-Concur – no controversy on the principle, there is some links to the measures here (independence and isolation).
        i. 5-6-2 Integrity of Data Loadable – agree should not be so descriptive, removed some text that you applied to do that.
        ii. Action - Rewording
        iii. Some way - > a means
        iv. Consider attacks rather than errors

v. Procedural and technical measures
vi. Proposed rewording to give to Michel and review with group:
vii. Principle 2 – Integrity of Connected Equipment
viii. Architecture Principle 2:
ix. 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.
x. Rationale:
xi. Ensure basic trust assumptions.
xii. Additional Information:
xiii. The integrity check should consider intentional attack as well as errors. This can be achieved through technical and/or procedural security measures.

- High 94-95 – agree with the resolution
- High 294 – Detection and restoration – accept the proposal but added some additional text around the complexity for fail secure, fail safe takes precedence over fail secure – Agreed and closed
- High 300, 301, 302, 350 – clarifying security barrier vs security measure
    i. Dave – collection of measures to defeat one threat or provide one layer against multiple Threats
    ii. Pat – unity
    iii. Dan – consistent with usages
    iv. Pat – make sure we carry this definition
    v. Ravi – defined in document
    vi. Michel – might need to adjust definition
    vii. Discussion around security measure (at functional level) security barrier is more a feature of the architecture – DJ
    viii. Need to have a definition – see page 10 and 11
    ix. Glossary definition in glossary needs to be defined – should come from the architecture group
    x. Action - Architecture group to update definition as well
- High 351 – Security Architecture Principles
    i. Was discussed with the group and the commenter and agreed to keep principles
    ii. Closed
    iii. General comment must and shall need to be revisited
- High 483 – Decomposition of Assets in Security Architecture
    i. Editorial group accepts suggested resolution

8. Assets committee (1 NC, 6 H) – P Watson
    - One Non-Concur – 2-2-1 - agreement has been reached with Boeing – need to change ‘must’ to ‘should’ in the resolution
        i. Is guidance – what you should follow, or help you understand – consideration – PM
        ii. Boeing NC on 2.2.1, Boeing commenter good with proposed rewording
        iii. Change must to should

iv. Martin provided more context as he discussed with systems AR who made comment
v. Is there a feedback loop in DO-326A between safety and security? Most say yes, Michel says loop is one way and the other way is implied (i.e. security does not feedback to safety though implied)
vi. Stefan – text is misplaced, should be having this discussion in 3.3, Romuald agrees
vii. Philippe – does this mean revise 326A?
viii. Dave – maintain ARAC report as closely as possible
ix. Action – don't change 2.2.1, address in 3.3, Phil, Martin and Siobvan to discuss with commenter offline and resolve
x. There needs to be another round with the commenter that the change is not made and the comment is covered elsewhere.

- Section 2-2 – 384 and 198 – 'remove 'in many cases 'resolutions accepted
- Section 2-2-3 – evaluation and connectivity should consider all systems
- Section 3-1-1 – any interfaces, changes the text a little – as there may be other means – Closed
- Section – 5-3 Three High Comments – concern that an asset is not a security measure – subgroup disagrees, embodies added and the rest of the comments were rejected. – Closed

9. Document Scope committee (1 NC, 2 H) – S Schwindt
    - Non-Concur Guidance and considerations are not thought to be separate enough
        i. Section titles should indicate whether guidance or consideration – suggested to move out sections 2-5 and 3-7
        ii. DP – are there any RTCA/EUROCAE definitions for guidance and consideration. EASA use 'should' for acceptable means of compliance
        iii. Shall, should and must conversation must start early
        iv. Romuald – this is an EASA acceptable MOC, EASA uses should when not accepted MOC
        v. John – a lot of shall statements throughout document, haven't searched for must yet
        vi. Anna – these are voluntary industry standards and guidance
        vii. Philippe - From beginning, understood authorities would regard document as accepted MOC
        viii. Dan - Should is more tightly defined, doesn't have same implication as 2 years ago, committee needs to review
        ix. Varun – where applied, look at technical content
        x. Martin – definitions up, are we making the should the shall?
        xi. Stefan – we have been deferred clean up action for 2 years
        xii. Philippe – keep should in both sections, guidance more prescriptive than considerations
        xiii. Stefan - Writing what to show so you can comply with rules, need to justify if you do different, also giving good practices for industry to follow whether for certification or otherwise

xiv. Should, shall and must needs a clean-up and that is an action
xv. RS – would promote the use of should, which means the document would then need another review of the whole document
xvi. STEFAN proposals
    1. Section 2 is guidance to understand regulations
    2. Section 3, 4, 6 is acceptable means of compliance
    3. Section 5 is best practices for industries – considerations
xvii. Waiting on proposal from Cyrille

- High - AEH – not sufficiently covered – action to review the use of airborne software, and every use of software appropriate. Doesn't the scope of the document already do this – could redefine to include complex hardware.
    i. If something could be misunderstood – then should be amended
    ii. Action - Editorial group should review and propose way forward

- High - Manufacturing Phase
    i. Proposed to reject the document as this document is about achieving certification and not the POA. Not about the manufacturing phase in general but more about production
    ii. Not part of the scope – and agreement that comment can be rejected

10. Example Methods committee (2 NC, 13 H) - C de Castro
    - Most NC's and highs are associated around Appendix F
    - Siobvan – most came from me, rewrite of appendix F added last minute in December before FRAC / OC, prioritized that as a review
    - NC was an overall NC that unless we address appendix F comments, revert back to previous version (DO-356 Rev New version)
    - Confidence we can get appendix F ready for publication
    - **Action – Siobvan, Claudio and Dan to discuss this week and close out all the NCs and high**

11. External References committee (1 NC, 0 H) – M Messerschmidt
    - Non-concur – 544 – text proposal to allow all choices
        i. Resolution agreed and closed
    - H-305 – disclaimer to be proposed and agreed with commenter
    - H- 696 – lots of repetition and tough to read, agreed but not sure what can really be done in the timescales
        i. Discussed comment that document reads like a collection of white papers, repetition, tough to read, want to see DO-178 structure
        ii. Would like to implement, but we are running out of time
        iii. Yes, it is a collection of papers from different authors

iv. Reject based on time constraint, try to address in another revision?

- H- 1050 and 1308 are around formatting
    i. Comment – ordering is not considered logical, doesn't align with other standards and how they list their objectives
    ii. Move security risk assessment to the front
    iii. Keep rest in the current order
    iv. Some topics don't align to a section, for example refutation
    v. Proposals are that numbering in the document will be fixed, and letter prefixes may be useful. Maybe re-order the risk management section. Move security risk assessment upfront.

12. Level of Threat committee (1 NC, 2 H) – A Waller
    - NC 604 – open ended – proposed text agreed to – Comment closed
    - H – 437 – minor changes to text – Comment closed
    - H – 1089 – Needed clarification – and changes around to required minimum – Comments closed

13. IUEI - Gilles
    - Spoofing means something different in German, be careful of terms
    - Varun – keep to scope and TOR
    - Dan - GPS signal that causes software to freeze – yes that is within our scope, it is interference
    - Varun responding to Cyrille – two other committees are working on this, the wireless and the wired to LRUs, jamming not in scope
    - Martin – are we taking issue just with term jamming?
    - Dan – intent to exclude analogue jamming, keep digital aspects
    - Steve – they have to deal with it
    - Dan – they have to deal with solution / implementation
    - Any digital signal is electronic interaction
    - Philippe - GPS was not in scope because it fell under government services, but now it is in scope because it is a specific entry
    - Cyrille and Dan - Exclude specific wireless systems. Don't exclude all just because of one case
    - Stefan - Specific wireless signals trusted, then don't need to do anything else with them, then address other cases
    - Martin – clarification – trusted or out of scope due to government sources?
    - Michel – I would include spoofing of wireless signals
    - Dan – add GPS to trustworthiness section as government service that we trust, from a government standpoint as opposed to a technical standpoint
    - Keep jamming
    - Steve – don't include bold text, what happens with the next technology that comes out and the next?
    - Need check on accuracy of this IUIE discussion

- **Action to Gilles – discuss offline with people with conflicting opinions and come up with rewording**

14. Risk Acceptability committee (2 NC, 2 H) – P Marquis
    - NC 572 – provide guidance unacceptable to acceptable – need principles for major, hazardous, this also applies to section 4 – what is the exact change being proposed.
        i. Bullets should be replaced below table and refer to section 4.4?
        ii. Disagreement to just have this in section 4 – as this section is the regulatory considerations, and this is the minimum requirements
        iii. The issues are consistency with section 4
        iv. Looking at risk acceptability matrix
        v. Stefan - Matrix is minimum, chapter 4 is what the industry thinks
        vi. Dan trying to clarify what is considered guidance vs. required vs. considerations vs. means of compliance regarding matrix and chapter 4
        vii. Martin - Single security measure isn't going to protect you against the scope of threats
        viii. Sam wants a note below matrix that deals with Hazardous and Major
        ix. First bullet
            1. First bullet to stay as is acceptable means of compliance
            2. Just need to reference 4-1?
            3. Proposal needs to be made by the group
        x. Second bullet is objecting to the term security assurance level
            1. Proposal - The level of threat reduction is based upon the security assurance associated with the security measures
        xi. Action – no resolution yet, side conversations needed

15. Risk Assessment committee (1 NC, 14 H) - P Marquis
    - NC 445 – Not resolved yet – as the comment is not understood – Comment was explained by Claudio
        i. Looking at threat consistency check figure
        ii. Claudio – Differentiate between aircraft level vs. system level
        iii. Michel – postpone comment
        iv. Dan - How you divide and classify threat conditions
        v. Detailed – multiple threat conditions associated with same asset
        vi. Philippe, talking about defining risk, not asset
        vii. Dan – how much threat "allowed", it's a balance
        viii. Claudio - Flight control systems, need to pass through other systems, how do you manage change of threat conditions to reach the target
        ix. The subgroup needs some time to work on the proposal
    - H - 456, 458, 835 – suggested resolution agreed
    - H - 442, 443 and 444 – proposed wording needs to be reviewed – slight change "severity of a threat condition"
        i. Editorial group needs some time to further consider this

- H - Group 450, 452, 455, and Group 451,453,454 – New suggested wording has been made to the second that means first group is superseded – Comments agreed
- H – 840 – the group disagrees as it would mix and make things less clear
    i. Dan - Assure that you meet requirements
    ii. Stefan – what is missing is assignment
    iii. Dan – agree, however don't believe in SAL
    iv. Martin - At end, risk assessment includes security assurance levels
    v. Dan - Part of verification, not risk assessment
    vi. Not same as independent assessment
    vii. Martin OK with what Dan said
    viii. Stefan – don't accept comments (even NC) that do not have a proposed resolution
    ix. Need to see proposal to be able to agree to it
    x. Dan questioning location of discussion on assigning SAL
    xi. Philippe - To mitigate risk, change architecture or apply security measures to reduce level of threat, measures require assurance assignment
    xii. Michel – different between assessment and evaluation – if you apply SAL, you are reducing level of threat
    xiii. Would like to keep out of chapter 3
    xiv. Martin – security measures binary, either they work or they don't
    xv. Editorial Group needs to make the proposal and for Stefan to review

16. Security Scope committee (1 NC, 11 H) – Phil Watson
    - All comments closed except the STPA definition, Claudio to provide amended words

17. Terms and Definitions committee (2 NC, 6 H) – John A
    - No slides with proposals, went through filtered spreadsheet
    - 580 – Took the definition from 202A - Closed
    - 573 - Note has been produced which was discussed at the meeting
        i. Comment 573 has text we discussed this morning, how we define shall vs. should vs. may (etc.)
        ii. 80 shall statements and 40 (estimated) must statements in the document, and it is supposed to be guidance
        iii. RTCA documents have paragraphs on shall and must
        iv. EUROCAE also gives guidance
        v. John – not doing performance requirements
        vi. Varun – may be doing performance requirements from applicant POV
        vii. Title of table – performance requirements and test procedures
        viii. Varun – shall is used for requirements
        ix. Steve – FAA defines shall as imperative
        x. John – want to leave it in the hands of the committee

xi. Michel showed resolution, that we should avoid "shall" and "require"
xii. Committee agrees, now we need to apply to rest of document, use should in document as it is guidance
xiii. Dan - Need consistency
xiv. Varun – objectives should be "shall", otherwise how are you going to meet them?
xv. Michel – objectives already use "should"
xvi. Proposal is agreed but it needs to be applied to the document – **actions is to look at the musts and should**

- 1213 – Sub-item – another proposal is to replace with 'component' – agree with the editorial group proposal
  i. Defined twice, no use for multiple item except 1.6 and 5.2
  ii. Recommend remove definitions in glossary and 1.6, leave what's in 5.2
  iii. Stefan – propose using "component" instead of "sub-item"
  iv. Dan – what granularity do you make your assignments?
  v. Varun – what's wrong with keeping in glossary?
  vi. Michel – definitions are different
  vii. Dan – change glossary to agree
  viii. 2 assurance levels in an item
    1. DAL -> not possible
    2. SAL -> possible
  ix. Resolution – edit sub-item definition in glossary
- 1212- change the definition of Security Barrier – agreed
  i. Security barriers came up again, already resolved this morning under architecture group
  ii. Dave – if you got agreement from commenter, not need to spend time on it
- 475 – Agreement has been reached

18. Certification committee (6 H, 20 M) – Stefan S

- Comments 1042, 125,124
  i. Guidance in chapter 2 on certification and evidence is wrong
  ii. Fix or remove
  iii. Need applicant to be able to use
  iv. Cyrille (from before) – applicant already knows cert basis, not going to learn that from our document
  v. Options
    1. Remove entirely
    2. Correct guidance
  vi. Varun – add statement that tells you to look up info on cert basis
  vii. Go with second option, correct guidance
  viii. Section 2.3 on STC needs to be changed
  ix. Steve – don't get to vote yourself off, need to provide justification for why you don't need to do the STC, not just because you don't feel like it
  x. Where is the disagreement?
  xi. Dan – if you take it out, others might take issue with you taking it out,

don't get too radical because you don't want people who were happy with the document to then be unhappy

xii. Stefan – lines of section that EASA wants to be taken out are from EASA
xiii. Committee agreed to remove two paragraphs per EASA question
xiv. Related comment from Airbus, TCDS and cert basis
xv. Committee agreed to remove first 4 paragraphs to address both comments, can start on 5th paragraph, "Prior to every modification…" and section still makes sense
xvi. Mitch - Assuming reader is familiar with this topic (aviation security certification), should we add a sentence regarding this assumption?
xvii. Stefan – no new comments
xviii. Varun – discussions still related to last comment, want to make sure we provide link and context
xix. Michel – OK for commenter, came from Airbus

- 200 – SSCG needs to be deleted or provide a definition, aircraft is also missing, so would need to be both, effectively its covered by the process document
    i. Boeing & Airbus do not use SSIG to produce the ASOG (or for any other purpose)
    ii. Embraer uses SSIG from their suppliers, however Claudio does not think additional detail or guidance on SSIG is necessary because the SSIG he receives is sufficient
    iii. Decision - Reject comment and refer to 326A / 202A
    iv.
- 776 – Dependent on Trustworthiness discussions
    i. Last comment in certification deals with trustworthiness, change it to trustworthiness editorial group

19. Measures committee (7 H, 8 M) – Martin C
    - Security Measure Relations
        i. Two options common mode approach – rewrite the definitions and examples
    - Discussing security relations options
    - Need to make sure we are not prescriptive on architecture and measures
    - Currently known + flexibility for something in the future
    - Recognize difference between safety and cybersecurity (think independent)
    - Need to continue discussion tomorrow
20. Adjourn

2 Tuesday, March 20, 2018

1. Administrative Remarks – Michel M / Anna vG 9:00am
2. Threat Conditions committee (4 H, 15 M) – Gilles D
    - Gilles presented the threat conditions high comments
    - H-1304 - about using the same definition as the safety impact, proposal is to change and use the text of 25-1309
    - Discussion around there are various versions of AMC1309, and removing the comment
    - Summary

- Accept the proposed resolution with a foot note that it is from a certain AMC and change the word definition to Reference definition
- H-423 concerns a reference to Appendix E3, the wording implied mandatory and just want to change it as Appendix E.3 illustrates an example
- H-1273 – Threat conditions identification and evaluation
- Resolution was agreed
- H-1216 – Threat conditions
    i. Martin - vulnerability to limitation, if you have a security measure with a vulnerability, then it really doesn't help you as a security measure
    ii. Varun - Limitations section on any airworthiness doc, design deficiencies
    iii. Dan - A vulnerability is a weakness, can be the same thing
    iv. Discussed IP filter example
    v. Dave - Threat condition identification, this is the place to discuss vulnerability of security measures
    vi. Michel - Don't introduce new terms in this document, a security measure may protect against one attack but open up a vulnerability to another attack
    vii. Gilles D. – doesn't belong in this chapter, subgroup does not agree, propose resolution in security measures chapter 3.5
    viii. More discussion, still disagreement on whether or not to accept proposal
    ix. **Action to Gilles – discuss with others offline and come up with another proposal re: 3.5 high comments**–
- H 3-4-1 Threat Scenarios
    i. Philippe does not accept proposed resolution for 3.4.1 high comments
    ii. Implies security measures and threat conditions do not belong to path
    iii. Michel – what is included in a threat scenario? Not always described in one structure
    iv. Gilles D. - Asset and vulnerability, not yet decided to build security measure and threat condition, don't necessarily have view of threat condition
    v. Consensus was agreed with PM on the comment resolution

3. EASA joint safety/security view on the SAL/DAL - Cyrille R
    - Want a common position on SAL and DAL and how they can work together
    - They held a meeting with senior experts in safety and security
    - The security assurance level (SAL) defines objectives to provide a classification in line with the level of confidence required for the protecting against intentional attacks on aircraft systems
    - Some activities are reusable from DAL and SAL and does not require to redo those activities
    - SAL will allow measuring how DAL activities contribute to the security and to know when enough is done on security
    - Question from Varun – How is SAL going to measure and tell the system guys what they need to do
    - Down to the objectives associated with the SAL
    - Varun – probability associated with each level

- Stefan - Has probability, function, done to certain DAL -> that's where things end for a system engineer
- Requirements done
- Cyrille is saying the same thing for security
- Answers Varun's question
- Dan – don't have a secure system, rather you have a system that met the requirements
- Stefan – both DAL and SAL, don't treat as completely different, check boxes in both columns
- Cyrille's conclusion – DAL and SAL are not opposed, do supplement to each other, and are both aiming at the safety of the aircraft and its systems
- Most people in room agree with presentation
- Dave – I think this presentation helps address some NCs
- Philippe – SAL complements existing safety process
- Michel - Defines the what and not the how, the how is up to the applicant

4. SAL/Assurance/Objectives discussion – Dave P / Michel M
5. Security assurance decision matrix
6. Should ED203A allow for all supplemental and independent approaches
    - Should allow for both then down to authorities
7. Should ED203A define the complete set of compliance objectives for all applicants
    - Dan - We developed objectives all summer, are we resetting?
    - Michel – No
    - Dan – single set of objectives doesn't work for everyone, looks more like independent rather than supplemental
    - Michel – should enable all approaches
    - Philippe – may have same view of overall objectives
    - Dan – issue is the "packaging"
    - Michel - Applicants should have common set of objectives
    - Patrick – This is a "should", consensus that we would like one set of objectives for all
    - Dave - Table vs. text, don't need to solve right now
    - Doesn't let you package easily
    - Patricia – actually there are three kinds of objectives
    - Security
    - Pure DAL
    - Overlap
    - Dan - Supplement, choose appropriate DAL, etc.
    - Martin - That requires direct mapping from SAL to DAL
    - Dan – no, these are the ones that are common, these are specific
    - Phil – easy to do for two highest levels (A and B), but not clear on rules with SAL for other DALs
    - Need check on this conversation

- Michel continued presentation
- SAL is not a company approach, it is something that all can use
- No way around defining some levels
- Looking up papers over time, Dan once proposed security related assurance levels, perhaps someone else has an idea, however don't want to discuss naming conventions
- Discussed interpretation of ARAC report
- Patricia referenced table, security specific assurance objectives shown
- Varun - Started with 3 levels of software and went to 5, far less headache if we could do one to one matching
- (True, but then why bother with SAL if you are duplicating effort)
- Disagreement over workload on supplemental approach vs. independent
- Supplemental approach needs to be less work, otherwise why use it
- Do it wrong -> duplicate effort
- Disagreement on the structure and application

8. Should ED203A define levels to distinguish different amount of rigor – Yes
    - Need to assure nothing is done to prevent either approach being conducted
    - RM - So it's really about adding additional objectives so what is the difference
    - STEFAN – the problem is around how you apply
    - DJ – Work over the summer – on what the security specific activities were
    - Patricia – mismatch could be around what is required
    - DP – the issue is around the packaging
    - PM – What about the fact that at the item level the DAL and SAL will be different at the item level
    - DP If they don't have the equivalent level of impact – it is really hard to do equivalence
    - Varun – would be far less of a headache – if we could do a one to one compliance -= five levels

9. SAL committee (9 NC, 19 H) – Michel M
    - Assign Mitch Trope as moderator to ensure people in room are not talking over people on the phone
    - Help needed to French speakers – check on status of metro strike scheduled for Thursday to see who is affected and for how long
    - Gilles D. – strike will affect entire metro system
    - Anna – cabs and Uber not affected, but allow extra time as they will be popular and traffic will be worse
    - Back to presentation
    - 11 NCs for SAL, all answered
    - 3 NCs disagree with assignment principles -> came up with new set of principles to replace them
    - 9 principles, principles 2 through 6 optional for system level

- Added "…the complete threat scenario is contained in one system or…" - would apply to new principles 1 through 3
- Question to Siobvan – If we delete "It is recommended to have two independent, diverse and isolated security measures in each such threat scenario," are we covered in architecture section? This SAL assignment principle pertains to aircraft level threat scenario that leads to a threat condition with hazardous severity, SAL 3
- Martin – issue papers and special conditions require layered defense
- Siobvan – architecture defense-in-depth section says you need two diverse security barriers, however, it does not specify DAL or SAL
- Issue papers and special conditions don't identify DAL or SAL either
- Stefan - Write with intent of rule
- **Action to Siobvan/Michel – even though there is coverage in architecture section, be more explicit and move sentence to 5.6.1 additional information for defense-in-depth principle**
- Discussion around SAL 0 and the proposal is to remove SAL 0.
    i. Looking at SAL 0
    ii. Martin – clarification, does SAL 0 means security for business reasons only?
    iii. Stefan - Think FDAL E
    iv. Will need to revisit NC comments from Chuck in afternoon when he's on the phone
- 5 comments that have been rejected by the commenter
- 613 SAL in DAL E
    - Resolution regarded as restricting acceptable approaches
    - Varun wants to understand tailored SAL for legacy
    - Phil - What does rejected by commenter status mean?
    - Michel - Means rejected proposed resolution
    - Rejection due to restricted approaches that were acceptable
    - Dave - If we follow what Cyrille said earlier, if we pull in DAL to a security solution and get to DAL E equivalent, you don't have a process, how can you take credit when you required nothing of it?
    - Martin – Boeing position – if you apply objective in SAL, then you've added something to it. We look at DAL E as min requirements that I need something, but I'm not taking assurance credit, but needs to be something to protect the aircraft, doesn't change DAL of system, but need to meet security requirement on system and verify
    - Steve – only add requirement for safety implication. No safety effect means no requirement
    - Michel – no safety effect due to failures/errors is different than no safety effect due to attack
    - Philippe – safety effect due to IUIE
    - Romuald – if we follow your philosophy (talking to Steve), every system talking to higher level system should be high level
    - Varun – don't make it a higher DAL

- Martin – agree, doesn't have to be higher level, however, security architecture, current SCs says we authorize access to aircraft, how do I do it if systems on perimeter that are DAL E? How do I know that the entity is authorized if there is no security?
- Steve – SAL 0 mapped to DAL E
- Michel – we do have certified systems at software level E but there are security measures, why is this not possible?
- Cyrille - DAL meant for safety, not security
- Claudio – if security measures fail, no safety impact immediately, so we can assign a SAL different from 0 to a security measure in a system that is E
- OEMs (Boeing, Airbus, and Embraer) in agreement
- Martin – precedence already, Embraer and Boeing agree, approved by FAA and EASA, credit to DAL E in cases, why is it not acceptable now to the level of a NC? What has changed?
- Varun – EMI requirements, level E should not interfere with rest of airplane and catch on fire, certain requirements in place that E has to meet to get onto airplane, Martin said why can't we add security requirements like EMI requirements? Don't have an answer
- Need to continue conversation after lunch
- Stefan – safety related to function, adding security does not change function, there are IFE systems with DAL D power supplies to protect against fire, protect function, safety measures where function occurs, security measures in chain of attack path
- Michel – don't see blocking point in applying document, up to authorities in what they accept
- Steve – answering Varun, security measures are intended functions in system
- Romauld brought up ARAC report, we are wasting time on this topic, we already have examples and precedence
- Martin – intended function, can also say implement security on non-safety system to prevent interference from other systems, don't want to limit
- Patrick – propose capture in text that historically DAL E systems not considered for safety security, but as negotiated, applicant may implement security features to appropriate level with authority, room to negotiate
- Dan read from ARAC report to clarify points of discussion896 SAL has no relation to DAL/impact

10. Break for Lunch
11. TAC Discussions J Moreaux
    - Tomorrow at EASA TAC meeting, one of the issue to be addressed is security event management
    - Logging from vulnerability management to incident management
    - A few years from now, 2020, we will have rulemaking 720 (EASA ESCP rulemaking)
    - Acceptable MOC for ATM and other stakeholders, if developed correctly, can be applied to aircraft and other organizations
    - Workshop last May, discussed WG-72 items

- If there is a need to raise other issues, let Jean-Paul and Clive know so they can bring them up during the TAC meeting
- Clive handed Jean-Paul a list of discussion items from joint EASA and EUROCAE workshop, Stefan put it on the screen
- Logging separate from vulnerability and incident management
- Risk assessment methodology – Jean-Paul referred to TAC STORM
- Maintenance security
- Michel – if we agree to ED-203A, there will be new activities for WG-72 this year
- Anna – three activities, one requires extension of deadline
- Formal update of TOR
- Streamline decision making process
- Upcoming documents:
    i. ED-xxx Guidance on Security Event Management
    ii. ED-201A AISS Framework Guidance Document
    iii. ED-204A Information Security Guidance for Continuing Airworthiness
    iv. ED-205 Security Certification and Declaration of AIM/ANS ground systems – published end of 2018
- EUROCAE call for participation
- Stefan – any other ground equipment you want to cover?
- Jean-Paul – need to convince that they are ready to cover those, upcoming work on cameras and scanners
- Every stakeholder has own way of doing risk assessments
- 201 needs to be reopened, as soon as 203 is done, there are inconsistencies between the documents, need a limited transaction log or tasks to make them consistent and focus on individual sections

12. SAL committee (cont'd) – Michel M
    - Dan reread ARAC report excerpt
    - Steve – harmonized does not mean mandate
    - Clive – we want option to be able to do it, if Panasonic doesn't desire it, fine. However, if aircraft manufacturer wants it, we need in document the option to allow you to do it
    - Cyrille in chat window – agree with Clive 100%
    - Patrick – silence means agreement, now we need draft sentences
    - Martin – sentences already in doc, that's where NC came from, we can borrow ARAC report words
    - Steve – integrated approach, not possible. Parallel it is
    - Dan – I have seen it in both
    - Michel – what is done in practice and what is prevented by such a standard
    - Gilles D. – proposal, text that discusses current process between air framer and IFE
    - Phil – industry might become less safe if you put things in level E systems, should be some change control on level E where there hasn't been

- Michel – mandated by SAL, security measure on DAL E makes it SAL 1 automatically (SAL 1 or higher for security measures)
- Claudio agreed with Michel
- Varun – problem putting things required to function in level E system, don't do anything about level E, verify it doesn't catch fire or interfere with other systems. If you introduce new controls, you need to look at intended function. Would be changing 40 years of precedence. This is your document, a consensus document
- Changing industry processes as well as regulatory processes
- Can be done, but would like to explore other solutions
- Function vs. content
- Martin - IFE considered untrusted
- Dave – going back to when you put a security control in DAL E, it is SAL 1…DAL and SAL share objectives, so that means you are including SAL 1 objectives that might go beyond DAL E
- Cyrille brought up level C case
- Varun – level E case is the issue, looking at if there are errors that come through, is there an effect on the airplane, doesn't care if errors are intentional or not
- Martin – wireless access point example, take a WAP for crew use, authenticate and access
- Should the WAP fail, someone other than crew can access
- Doesn't introduce errors or cause safety effect
- However, now they can access other systems on the network
- Difference between knocking on your door and being in your living room (propagation)
- Failure of security control doesn't mean threat condition will be realized, malicious action still needs to go to next step
- Varun – controls housed elsewhere
- Martin – not true, some controls in DAL D and E
- Cyrille – that is a SAL objective
- Philippe - 2 assurance, safety (DAL) and security (SAL), through SAL you have confidence that security measures are commensuration with your requirements
- Jean-Paul – don't see different between security and safety because we do both for safety
- Address development errors as well as malicious
- Stefan - Can narrow down SAL to what's necessary
- Michel – question to Steve, can we address your NC without precluding the other positions?
- Varun to Steve – can you provide a resolution / proposed wording?
- Steve – or I can provide a dissenting opinion
- Michel reminding us that it is better to find common ground this week than to bring a dissenting opinion to RTCA PMC and EUROCAE
- No agreement on comment, Panasonic threat of dissenting opinion
- Dave – we plan to put document out in May and deal with dissenting opinion if needed

- Patrick – discussed how to include all views, to represent everyone, per ARAC, can we say if you implement security in level E, it needs to be negotiated with EASA and FAA
- Seems to represent everyone's opinions
- Steve – don't need to put that in document for people to negotiate
- Varun – FAA and EASA want a lot of this stuff worked out in document, less work to refer to document than to negotiate
- Moving on
- Chuck not on phone to discuss his NC369 – CR comment – pause
- 897 – Require partitioning to ensure isolation
    - Subgroup believes it is already covered in the document
    - Phil – against defining partitioning as there are many ways to accomplish
    - Dave – High SAL and low DAL, should have same level of rigor, give industry strong level of safety
    - Example – failure if you have high SAL and no code review
    - Don't want SAL and DAL to compromise each other
    - Stefan – what are the common modes, need to find a wording that there is an appropriate 'separation' between the two
    - Dave – Would like to see alternative words to independent isolate diverse – they are not concrete and practical enough
    - Michel – Isolation, independence and partitioning is one method
    - Dan – would like some discussion on common mode and we could point to those discussions
    - Michel – Need a proposal made – SS to prepare something on common mode analysis. You just need to justify common modes are acceptable
    - Stefan – common modes that can impact security? Partitioning can be OK in some cases and not others. Look at recent vulnerabilities where you can read memory from another section
    - Need separation appropriate for what I want to achieve
    - **Action – Stefan, Dan, etc. will work on proposed resolution wording to address GE concerns**
- 896 – SAL has no relation to DAL and impact
    - The proposal was rejected
    - Martin – we don't need 5 SAL for security, proposal – loose/variable mapping, don't want one-to-one mapping, want flexible on purpose
    - Varun – loose mapping OK but in practical terms it will cause more problems for the applicant
    - Martin gave example
    - Jean-Paul – aircraft is system of systems, may be last line of defense
    - If you fix too much, what you know currently, look at someone else's in case there is something that can be shared
    - To address NC "SAL has no relation to DAL / impact", Michel attempted a table mapping severity to security assurance
    - Martin – showing min required based on severity

- Philippe – table 2-7 is wrong
- Phil – fix this table, put SAL 0 for min (minor)
- Martin – some places where you do nothing for minor and no safety, but should have option to do SAL 1 and get regulator to buy in
- Michel – why include table in doc?
- Martin – compromise to help people having issues with applicability of SAL
- Safran – what about functions in serial and defense in depth discussion?

13. 1035 Security assurance assignments – proposal is to require full SAL compliance only for SAL 3 but allow for some tailoring for SAL 2 and SAL 1 on legacy situations

- Varun - Making a change, need to manage via that STC, not looking at entire airplane
- Stefan - Confusion about tailoring, if you make change, doesn't have to consider all our objectives? Cyrille concerned about change to legacy system and applicant thinking you don't need to do anything
- Should comply with all objectives which may not be possible for legacy system
- Martin – we have looked at legacy systems designed priors to SCs, and we have taken approach to how system was built, are there vulnerabilities, are there security measures, do penetration testing (refutation testing)
- High assurance systems by nature are typically secure
- Are there IP items we can't meet? Example – legacy doesn't do security logging, designed prior to that
- Not being able to log -> doesn't cause a safety / security issue
- Varun – what risk are you bringing to airplane? How are you mitigating?
- Stefan – change to legacy program, don't retroactively go through code coverage
- Noncompliance to objective – is it really a problem? Coverage though other activity?
- Do whatever you want is not OK from regulatory perspective
- Also don't want to burden applicant
- Middle ground?
- Michel – one suggested resolution from EASA and subgroup
- Subgroup agrees for SAL 3, but for SAL 0 through 2, need tailored
- Hoffman – need right language
- Varun – everyone is going to do the minimum, nothing more
- Steve – negotiations between regulator and applicant can result in tailored approach
- Use Steve's words as new resolution
- Martin – process question – some of us are pursuing delegation where AR is wearing regulator hat, does this mean negotiations with AR?
- Varun – AR cannot interpret FAA regulation
- What about Europe and EASA?
- Stefan – European equivalent only allowed to interpret minor changes
- EASA wants Baseline approach with specific tailoring

- Resolution – Dedicated tailored security demonstrations and evaluations can fulfil SAL objectives compliance. When some SAL objectives are not fully covered, complementary activities may be negotiated to reach the required SAL.
- 1054 – Some principles are certification requirements
    - Some principles are certification r requirements
    - Stefan – Intent was not to mandate SALs on all applicants
    - **Resolution – push recommendations into chapter 5, something good to do but not required**
    - Not required to be an AMC (Acceptable Means of Compliance)
    - Which chapters are AMC, industry guidance, etc.?

14. Chuck on phone, get to his NC
15. Will not get to high comments today
16. Romuald – need to get to logging, will be leaving tomorrow

17. 367 – Section 4-4 not required
    - Implication in 4-4 is that SAL is an essential concept for everything. It fails to show a strong relationship with safety and in his view it muddies the water. The issue is that it seems to be a mandatory approach and does not allow for the DAL approach.
    - So what else can be changed
    - Patrick – SAL definition groups objectives that need to be met
    - Set of objectives should be common between the independent and common approach
    - Will need to be discussed further
    - Jean Paul – Talk about objectives and then how then can be assigned SAL and DAL+
    - Chuck needs more time to consider this
18. Continued Airworthiness committee (2 H, 7 M) – Brian V
    - 191 – Disagrees with the proposed as Technical information would not expose details on security architecture. Technical information will be contained in the DAH provided operator guidance
        i. Can agree with the subgroup proposal
    - 276 – Agree with the subgroup proposal
    - EASA doesn't see impacts in near future
19. Logging committee (4 H, 3 M) – Brian V
    - 4 high comments
    - 103 - First one on standardization of logging format, change "should" to "may"
    - Second one is a Boeing comment, slight modification to response, "Maintenance messages may be issued when a system fails or when a maintenance action may be necessary…"
    - Discussion of whether we are talking about dispatch messages
    - **Proposal accepted**
    - 548 Maintenance messages
    - Martin – are all security message maintenance or are all maintenance security?
    - Dan – neither
    - **Resolution – delete maintenance messages bullet**
20. ADJOURN

3 Wednesday, March 21, 2018

1. Dave Pierce gave introductory marks
2. Security Assurance committee (cont'd) – Armelle G
    - 190 comments received
        - 7 non-concur
            1. 2 in proposal
            2. 3 in work
            3. 2 in linked status
        - 52 high
        - 85 medium
    - 377 - Appendix A1.2 Chuck
        - Linked to two other comments 375 and 376
        - Cyrille challenging security specific tags for 0-8 and O9.8, he wants to remove all security specific rags and move to the independent approach only
        - So first they are only specific objectives – no added value as all set to yes
        - On the second point – this column is not mandatory – useful to identify objectives that may be met by safety development, but some additional work is required, so should not be moved to the independent approach as useful for both
        - Michel – Did chuck agree or disagree – not been discussed, so park this till Chuck on line
    - 543 – Implementation Objectives – no criteria similar to DO-178, and is focused on coding standards
        - Proposes to delete coding standards or reference to a specific coding standard
        - Proposed resolution – was the set of standards used by an applicant can vary, so an accurate list for each applicant is not possible to create
        - Subgroup – proposes not reference some specific criteria
        - Stefan – should be the expectations of what the coding standard should bring. Coding standards should address vulnerabilities
        - Dan agrees to an extent – he has looked at this and the standards groups are still looking at this as it is a moving target and a general statement is all we can do at the moment
        - Chuck and Phil agree
        - Martin - If we are going to refer to coding standards we should provide a reference to what they are – so people know what is appropriate. Could keep open and let each applicant justify
        - Dan – DO-178C – each programme develops its own
        - Dave – agrees to add the note
        - Martin – Concern is that it is a moving target - e.g. DO-178
        - Stefan - Has not found a problem with DO-178, gets updated as you learn, feels notes should say what the expectations is
        - Michel – should say the set of security standards as opposed to set of standards

- Stefan – disagrees it should be one coding standard that satisfies security and safety – DO-178
- Martin – should describe what the expectations are
- Michel – Isn't this covered in 54
- Dan – no research is still on going
- Martin does 54 line up with 178?
- Siobvan – Coding best practices to reduce vulnerabilities
- Gilles – can we refer to CVE – Coding standard
- Phil – agrees with Siobvan suggestion, referred to DO-178 section 4-5. Last phase of the proposal cannot be met
- Varun – Has always been a personal thing so you don't want to hamstring anybody
- Dan – could say and refer to11a
- Proposal change line 54 change to reduce vulnerabilities and "The use of a relevant set of coding standards used by the applicant to reduce vulnerabilities during….."
- **Proposed resolution in 4.2.3 – "The set of standards used by an applicant can vary. The use of a relevant set of coding standards used by the applicant to reduce vulnerabilities during the coding phase is a key element of the security process and development of effective security measures and targets."**

- 607 – subgroup accepts the resolution proposed by Dan
  - Replace the sentence – resolution agreed
- 609 section 4-4-3-1
  - Suggested resolution was to remove 4-4-3-1 also proposed by 1037
  - The subgroups accept the resolution – room accepts it
- 848 – Chapter 4
  - Dave – Expectation that the existing engineering process would provide a lot of the assurance activities that are required. The words imply the process is distinct and he proposed a rewrite of chapter 4 supplemental method.
  - Michel – different views on how topics should be arranged
  - Focus on smaller changes
  - Stefan – avoid use of supplemental and independent in document as that is confusing for outside readers, otherwise more explanation needed
  - FAQ document?
  - Dave – affects use of SAL, also SAL does not have same number of levels and definitions
  - We don't literally use objectives
  - Discussion last year about having the supplemental and independent approaches work with each other
  - Keep tables and SAL, which is not meeting people's expectations for the process
  - Romuald – define security levels, essential to define metrics, otherwise document is useless
  - Philippe – supplemental approach, how do you characterize supplement, SAL

definition identifies full set, subset is DAL, but in end you need something to collect for the full set

- Removing SAL – what is your proposal to character supplement to DAL?
- Dan – disagree that it is requirement to have full set. If you have DAL and SAL, it is full
- Looking at guidance from TOR
- Martin trying to bring us back to original concern
- SAL defines security objectives you are trying to meet (Cyrille)
- Let safety do safety and security do SAL security objectives
- Dan – difficult to believe we should have two parallel requirements processes, would like to see this:
    - 4.1 objectives
    - 4.2 supplement considerations
    - Turn those considerations into objectives
    - We meet 4.1 objectives, we meet 4.2 objectives, then map to FDAL and IDAL
- Michel – where do we look at software, system, hardware, etc.?
- Martin discussed how Boeing shows compliance, security ARs need to determine if these requirements are met, software and system ARs are only required to show compliance for 178 and 254
- Stefan – this is more about how people develop things correctly, certification is only ~10% of this
- Claudio – his people want to know about objectives rather than direct mapping, as Michel said, would be difficult to map everything
- Dan to Martin – transition period where we are creating environment where ARs can find compliance for security
- Continuing…looking at cost, certification is more than 10%, people are taking extreme position rather than compromise when arguing these issues
- Security requirements need to be reconciled with other requirements, otherwise we don't have a system. Three categories:
    - Security specific
    - How do you map the overlap, i.e. tag and trace security requirements
    - Objectives that both processes are trying to accomplish
- People wording objectives, so it doesn't look that way!
- We have a middle position that allows for both processes
- Michel – what is middle ground? This document needs to meet regulatory needs. Then, applicants need to find a way to deal with objectives, and there are different approaches
- Provide as much detail as possible on how approaches work
- Phil – I started trying to map 178 objectives to what we have. After 15 min it's nearly impossible. Some are one-to-one. In other instances, there are many that map to one. Would take a while and would need to restructure SAL (significant effort)
- Ravi – last summer we spent a lot of time doing mapping (see Appendix B), went from 140 objectives to 22, and now we are saying that the objectives aren't granular enough. Confused – what is the plan? Seems like we are

going backwards

- Patricia – agree with Dan's three categories and proposal
- Dave good with what Dan and Patricia say
- Use objectives tables, suggestions for rewrite is appropriate, want SAL as a 5-level system, also want layered defense
- Objectives discussion this afternoon
- SAL definition remaining piece of NC comment
- Philippe – process is set of activities
- Jean-Paul – agree with Dan's proposal, however this is a significant amount of rework, need volunteers, circling to same spot
- Packages of objectives – this is where we are in agree, but process of how to meet them is where we disagree, eliminate in document and leave up to applicant to perform mapping
- SAL most obvious way, but applicants can do differently as long as packages are met
- Proposal is to not map and focus on the packaging
- Will revisit later, continuing summary of security assurance NC comments
- Martin – we had concerns on security tools objectives as well, don't want to require all to be qualified, pen testing tools come from all sources, how to identify if output is good or not
- Use multiple tools from different sources in case one has a vulnerability, you are still covered
- Also need analysis with testing
- No one tool is going to find everything
- Stefan – separate what tools we are talking about
- Tools that produce something that goes into aircraft (rather than test tools)
- Make sure tool is capable of doing what you would normally do manually
- Going back to testing (verification), need to be able to repeat testing
- Martin – if you generate code, agree, you need to qualify
- However, there are useful tools that don't have a datasheet
- Varun – Different levels of qualification for development tools vs. verification tools
    - Development – inject code in system, could inject a failure
    - Verification – don't inject code, could fail to detect something
- Prove intended function -> almost there
- Martin – how to prove intended function with hacking tool?
- Gilles D. – issue with stop criteria
- Patrick - Agree (with Philippe) that requirements don't cause limitation
- Gilles D. to Philippe - not objective of 13.3, not because we propose to deviate
- Michel – discussing multiple proposals
- Armelle showed two subgroup proposals:
- Keep an objective for qualification per TQL5
- Remove O13.3 and keep only one objective for vulnerability identification
- Stefan doesn't like option A
- Why is security so special where we need this?

        - Philippe - Need to be able to use any kind of tool, don't want to be limited by requirements
        - Gilles D. to Stefan – Non-regression activity doesn't belong to security
        - Martin – based on discussion, if it is being able to repeat a test and state purpose, it is doable because we have ability to do virtual imaging for test suite, keep image forever, tools we use can change quickly, but can always go back to virtual image and rerun test, even if tool at different version, doesn't prevent you from upgrading version
        - More discussion
        - Dave – feels like we are agreeing but objective needs rewording, requesting proposal
        - Added an option C – relevant tools that could fail to detect a vulnerability should be under configuration control
        - Stefan – we should be referring to DO-330
        - **Action to Stefan and Philippe to work through objective wording**
        - Removed option C after all
    - Moving onto high comments
    - Proposals for all, need agreement from commenters
    - Dave – if the commenter accepted the proposal, probably no need to discuss
    - Michel – speak up if someone has an issue with a comment proposal, don't need to go through every comment
    - Looking at 4.1.2 security refutation objectives
    - No resolution yet
3. LUNCH
4. Security Assurance committee (cont'd) – Armelle G
    - 363 – 4-2-6 Configuration management objectives
        - Cyrille wants to move but the subgroup wants to reject, should come up again in the objectives section
    - 35 – 4-2-8 – Remove compiler from the list of tools to be considered, this was rejected by the subgroup. Discussion has now been made with Mitch
        - Compiler in list of rules
        - John A. – should be removed, why do we need to list? How do you qualify compiler?
        - Mitch – configuration generation, not configuration management, but willing to remove list
        - Stefan – disagree with comments 884 and 881
        - Michel – proposal is to develop guidance to address these, address in another document / separate
        - Armelle – hardware tools not addressed in section 4.2.8, will need to consider them
        - Dave – forward resolutions to commenters to ensure they are in agreement, that is the process for all
        - Finished going through NC and high security assurance comments
        - Michel – try to address all comments all the way down to low by April plenary
    - 334 4-3 Agreed with commenter

- 1233 – 4-4-3 – Agreed with commenter
- 22 other comments need to be discussed within the subgroup
- 338 H Refutation objectives - All Refutation Objectives are the same from level 1 to 3 except independency required for level 3 & 2
    - Needs to be discussed
- 17 high comments with linked status – should be resolved by the non-concurs. SS disagrees 881 and 884 are tool qualification but a different aspect – noted
- 609 was closed today – so the resolution should be forwarded onto the other highs for agreement and concurrence

5. Objectives committee (6 NC, 21 H) – Dave P
    - Comment 123 – The committee accepted the proposal with a small change
        - This has been agreed
    - Comment 375 and 376
        - Martin - If you are only doing DAL and supplementing it fine, but if you go independent needs to be included so it does not get overlooked
        - Patricia – they are more mixed, and showed her table
        - Stefan – missing Chucks comment O9.8 – Integrity and specify – this applies to all and not just security measures. Disagrees with CR resolution but does agree it applies to all.
        - Need to wait for Chuck
        - Dan likes the start and the philosophy of the table, or do we have a forth section on general requirements
        - Martin do we still need this column –
        - Dan yes we do as it indicates that what could be covered by DAL process. Needs an explanation on the column, if we keep it in the document P proposes in informative and not normative
        - Include objective to tag security requirements
        - Martin – not my understanding, is it defined that way?
        - Patricia – keep in document, propose to put in informative appendix, not normative
        - Martin – rather it says common to both safety and security
        - Dave – helps with some other comments from this morning
        - **Proposal - Column that directly attributes to safety, security, and mixed**
        - **Action – make firm proposal with right words for columns**
    - 462 – section 4-2-2 Security Function Interfaces
        - Had a proposal accepted in the sub group, proposal
        - Gilles D – Is this related to security function before security requirement
        - Michel security function is aircraft function for security
        - Dan – security function is a security measure at aircraft level, and does not want to include a new function
        - For every function should be a requirement
        - Michel replace security function with security measure – DJ would agree
        - If the security function with a security measure does this resolve the problem, Embraer – probably not

        - Better to have something missing than something half a concept
        - We don't have a concept of security function – so just remove
        - Refer to designated function of security
        - **Proposal to change 3-5 to security measure are not limited but include functions dedicated to security and replace security function with security measure**
        - **Claudio to send proposal text to Antonio**
- 606 and 612 Committee accepts proposal resolution
    - Agreed and closed
- Significant number of high comments and work is still required here
- 1236, 1237, 1247 and 1264
    - 1236 Suggestion is to split, are there any issues if it is split, doesn't not solve the problem of what does independence mean
    - Patrick – Scope needs to be developed in concert and not in isolation, so should be working together and not independence
    - Patrick - Security scope doesn't need to be reviewed independently, rather in concert, need to be developed together rather than isolation
    - Martin – actual issue is what does independence mean?
    - John A. – this document is not in agreement with what we did on 178, two definitions in 178C, one with development and one with QA
    - Stefan - Two definitions, one from 178 (two if 178C, see above) and one from 4754
    - Varun – different documents use terms validation and verification differently
    - Guy who is coding is not the guy doing testing
    - Clive – break down topic into questions
    - Does security scope validation require independence? If so, change text
    - More don't think so
    - Mitch – in our case, it's review, don't need review independence for artefacts
    - Stefan – may want it for quality control, but do we need to require it? Big organizations can do it, small organizations not so easily, can't expect every company to have the personnel
    - Therefore, narrow it down to what is critical, and which require independence?
    - Varun – what matters is which require independence, not how you achieve independence
    - Armelle – not clearly explained, proposed additional notes
    - Gilles G. – not able to validate anything, small entities will have limited competences on security
    - Stefan - What is independence for assurance and verification? Global independence
    - Do not want to include requirements for personnel competence because then we would have to define, company process ensures you have the right people
    - Discussion of plan tomorrow – still metro service, but reduced to a third, and strike has already started

        - Chuck on phone – go to his NC comments
        - Michel – had another discussion this afternoon that may change Chuck's mind, Dan and Patricia's proposal of three kinds of security objectives
        - Agreed to leave it as is and not split
- 848 Solution to draw out method anticipated by DO326A
    - What do we need to do to resolve this
    - Need to go through the objectives that provides what CR wants
    - So a review of the tables is required with a specific mind-set, reviewing the tables into security/safety/mixed
- 896 - Dave requires a proposal definition
- 375.376 – If we break this down into three categories is that sufficient
    - Cyrille - The two items in 8-2 are not security requirements
    - Stefan They are security in that we need them to feed back into security, 178C only links about safety. We need to ensure other activities take into account security.
    - Michel If we have a third category that is mixed then this covers this
    - Cyrille – If there are things in work to go on that lines could be okay with this, so propose something and see if that moves the comments along
    - Dan in each case there are objectives where there is a link to security, and how they are hooked together
    - Martin – common or unique tags, but how to address mixed
    - Michel – security specific – is a unique objective for security
    - Michel – Mixed is another consideration that you need to consider
    - Dan Agrees with the intent
    - Cyrille – Sounds like it is heading in the right direction, but complication – if the reason for the objective is not unique it should be existing
    - Michel – As a working group – want to be fail safe, would rather impose objectives that may be redundant, rather than miss objectives
    - Martin – Having them redundant allows for both integrated and parallel be applied
    - Chuck – not proposing to remove objective, proposing to change the tag, remains there for integrated parallel process, doesn't feel profitable to work detailed proposal when other comment resolutions would supersede, defer this one
    - Cyrille happy to defer until see the new proposal that covers everything
- 377 – Should be relocated into appendix
    - Michel does not specify independence or supplemental approach. Normative should be applicable to all approaches
    - Stefan repeated what Cyrille stated earlier in the morning
    - Michel – Want to limit objectives to acceptable means of compliance
    - Michel – Regulators want one set of objectives
    - Cyrille That's fine but believes another problem will occur with the tables again
    - Refer back to the answer in 375

- 376 – O9-8
    - Cyrille difficulty he has is this is changing the development process, may not be invoked
    - Michel – Yes it may interfere with the development process, but it is a good objective
    - Dan – would like a regulator view – DO- it was worded as protection from deliberate corruption
    - Martin – Is this really out of scope
    - Stefan we should make reference to DO-200 and 355 where it is outside of the development side
    - Michel would keep the objective as it is
    - Stefan would prefer the security specific
    - Proposed resolution – write what is in scope in this document and to point to out of scope
    - Michel how do you want to address the out of scope
    - Stefan – would write in this document what is in and out of scope
    - **Stefan to propose a solution**
- 884
    - Stefan Not expecting any change in the document, running tools with known vulnerabilities. It is a concern, and not good for the overall ecosystem. DO-330 is probably the right place and refer to the appropriate committee so we can get the right balance that tools are okay
    - John Does not believe much chance of opening up DO-330 as it knocks on to 178C
    - Varun – related, if you open one you have to open the other, less independence than you think
    - John A. - Takes more real estate to qualify a tool than airborne software
    - Stefan – missed the point, problem is you have to freeze development environment, don't want to be stuck with windows XP forever for example
    - People running stuff on insecure OS vs. people spending a ton of money to qualify
    - More weight if committee says there is an issue rather than one person
    - Michel – Specific solutions to specific problems – none of this belongs to this document, but
    - Make a request to RTCA;/EUROCAE that goes to the committees to address the problem – resolution agreed
- 551 – Have received an updated comment has been agreed with the commenter - agreed so change to safety assessment process – need to check commenter agrees
- 1040 Has had an update – new proposal is to replace with electromagnetic disturbance – agreement but need to check that Cyrille happy with this – 2-2-1 line 40 **– need his confirmation**
- 1216 – Dassault Security Measures – group has proposed a resolution does Dassault agree. Agree with subgroup proposal

- 1304 – Change example definition and add a reference to the source. By a footnote to the example definition- Agreed and resolved
- 572 – Update has been received from Philippe and it is proposed to add something below the table if risks are not acceptable "being assigned security assurance objectives according to section 4-4-1)
- Stefan disagrees on grounds of acceptable means of compliance
- Michel it is a solution – the question is whether it is a good solution
- Sam – This is a pointer and helps people find solutions – sees no issue
- Philippe it is an example to make the risk acceptable, and 4-4-1 is the only section "additional options for"
- Stefan Still has an issue as it stops people providing an alternative means of compliance
- "We provide acceptable means of compliance in later chapters"
- The acceptable means of compliance for demonstrating risk acceptability are found in the relevant chapters of this document

6. ADJOURN

4 Thursday, March 22, 2018

1. Administrative Remarks
    - Michel Opening remarks
    - Intention is to go through all the security assurance comments
    - Outlook where we are and then tackle the non-concurs that are open, and then review the high comments that have a proposal
    - NC – half way closed
    - 70 comments to be reviewed today (NC/H)
2. Additional SAL/Assurance/Objectives discussion – Dave P / Michel M 9:05am
    - 573 – Michel Use of should, shall, we had an agreement to review the use of should in the document. In the normative sections, MM has had a look and in general most of the use of should is considered correct. Honeywell agrees – Agree closed
    - 1206 – Considerations and guidance – Stefan – it's in work and hope there is a solution today
    - 575 – SAL assignment principles – move the recommendations of the hazardous case to chapter 5
        - Philippe – has a further comment – can security protection be added in the principles in SAL 0 - Agreed
        - Is the resolution acceptable for the 5-6-1 additional text concerning hazardous.
        - John A - Does security protection need to be defined
        - Michel does not feel it is required
        - Phil – should be independent, diverse and isolated
            1. On every aircraft-level threat scenario that leads to a Threat Condition with Hazardous or higher severity should include at least two independent diverse and isolated security measures
        - John A – This is not required in the risk table – two measures for hazardous

- Michel Section 2.7 – to accept risk in catastrophic – two measures
- Philippe Section 5 – is best practices so that is why there is a difference
- Agreed – with the resolution – Closed
- 576 – also closed as linked to 575

- 613
  - Last proposal was rejected by Airbus
  - Proposal is to add a statement. "New certification processes would need to be developed to require review of items that embody a security measure is required for aircraft safety".
  - New wording – not agreed to
  - Overall, disagreement between OEMs and suppliers / system manufacturers
  - Mitch - Need to include something about No Safety Effect (NSE) and be specific
  - Martin - Security impact but even though NSE
  - Philippe - Need to focus on safety impact for this document
  - Siobvan - No immediate safety impact, but could cause later safety impact via propagation
  - Martin – architecture
  - Stefan - If OEM from architecture reason needs higher SAL for DAL E box, follow process. Also business case
  - Mitch - 1309 reduction in safety markings as consideration, failure of security measure -> reduction in margins, need faith in underlying design of security measure where it won't cause reduction in safety
  - Stopping attack at edges, need to allow for review of changes, don't sweep level E under rug
  - Dave – multiple layers of threat condition, threat condition itself has severity, implementation of mitigations must rise to that level of severity, can't fail to protect threat condition it is supposed to protect
  - Don't care if someone gained access unless it causes safety effect
  - Gilles D. – can't divide threat conditions, choose SAL because for me, SAL addresses safety and other impacts
  - Michel – I'm not hearing new positions, let's stop for today and think again for later
  - Patrick requested Phil restate position
  - Martin – agree with Mitch that control in NSE equipment needs configuration control before implementation, at Boeing, no matter what DAL, goes through change process and Design Approval Engineers (DAEs) assess change
  - Use SAL to determine if security measure is functional
  - Requirements, verification, and testing
  - All we are doing is asking that you use SAL, it limits amount of document you do, want to remind you of ARAC report, suggests how to take credit for security controls in DAL E

- Care about this, if someone hacks an airplane via a DAL E system, it's bad for OEMs, suppliers, and regulators
- Cyrille (also from chat) - I just had a discussion this morning with EASA safety senior experts and they do not support the need to associate the DAL to the security "level", although they contribute to safety. Take again the example of the cockpit door. DAL C for safety purpose (crew need to be able to unlock in case of emergency). No DAL for security at all, although the security risk is CAT.
- Dave – table issue for later, each side illustrated their concerns, this doesn't have an immediate solution
- If we use Phil's language, is it easy to do what you want to do as long as you negotiation with authority?
- Do we need the authority to make a proclamation to handle this the right way?
- Phil - Not opposed to rewritten sentence, but it doesn't do enough to address concern, will think about it and write another proposal
- Cyrille R chat comment - shall I present the slides from Tuesday? I just had a discussion this morning with EASA safety senior experts and they do not support the need to associate the DAL to the security "level", although they contribute to safety. Take again the example of the cockpit door. DAL C for safety purpose (crew need to be able to unlock in case of emergency). No DAL for security at all, although the security risk is CAT.
- Dave P – Lot of discussion on this issue, each side has expressed concerns – and no immediate solution
- Phil W – It might be possible to merge the airbus proposal, PW to look at this to try and achieve a solution.
- **Action PW, MT, MT C Rosay to work out another proposal**

- 1054 – Changes the proposal slightly but need feedback from Laurent
- 14 Certification
  - Comment has been proposed by the working group. Is there any objection to the proposal? So adding a statement not a note - Agreed and closed
- 1206 – Document Scope
  - Resolution concerning acceptable means of compliance and consideration
  -
  - Amend Chapter 1-3 How to use this document
  - Need to specify what is guidance material, acceptable means of compliance, considerations, etc.?
  - Dan – we have one normative appendix, so we should extend this text to discuss appendices as well
  - Philippe M feels in section 3 and 4 some text is considerations
  - Stefan S – What sections 3 and 4 are considerations
  - Philippe M Section 4-4-3 – Move to chapter 5
  - Siobvan N to include 4-4-3 in Chapter 5
  - Stefan S – Needs inputs on what sections of 6 are applicable
  - Michel M – Could swap 5 and 6

- John A – Best Practices –is that a good term
- Varun – looked at a best practices document with less rigor
- John A. – better term than best practices?
- Order of chapter 5 and 6 proposed to be swapped. In other words, architecture will now be chapter 6, the last chapter before appendices
- Opposition to that, don't want to change document too much
- Michel - 4.4.3 Security Assurance allocation within the Aircraft should be a new subsection 5.3 Decomposition of Assets in a Security Architecture, make it 5.3.1
- (4.4.3.1 deleted, so 4.4.3 is very short)
- Stefan S – This document also contains considerations that are not guidance an d acceptable means of compliance
- Michel M 6-1 Considerations – 6-2 AMC
- Philippe M - Agrees
- Agree Leave chapter 5 and 6 as they are
- 4-4-3 move to Chapter 5 – as 5-3-1
- Ravi – Air you sure maybe 5-4 and 5-5 is more appropriate
- Philippe M feels it is appropriate for 5-3
- Move it to 5-3-1 and add a sentence to say defence is depth is discussed in detail later in section 5-5
- Also, make references to/from 5.6.1 defense-in-depth
- **Action to Siobvan – make the changes discussed, putting 4.4.3 into 5.3.1 and making the appropriate references to 5.6.1**

- 77 Architecture
  - New proposal was made
  - Mitch is in agreement
  - Resolution agreed and closed
- 104 Appendix A
  - Concerns the use of SAL in the Note
  - Stefan S – Has the note been deleted with the principals
  - Subgroup accepted the proposed resolution, its only a clarification
  - Resolution Agreed
- 263 Appendix
  - Resolution agreed
- 277 Security Scope
  - Agreed with the resolution
- 278 Security Scope
  - Agree with the resolution
- 279 Security Scope
  - ANSP means something different in the USA to Europe
  - Varun- All of our government sources are inherently trusted
  - Michel M – Agree with the resolution but spell out ANSP
  - Editorial for ANSP – we spell out in the document
  - Martin C Where is the baselines regulatory and international standards

    - Dave P – You have to state all of them and they are negotiated
    - Michel M – This is to help you define your security scope
- 292 SAL
    - Security Assurance Level – referring to legacy, and hence we start with the products and systems as we don't have assets
    - Gilles G - Romauld S may have changed his mind – defer the comment
    - Action – SAL group to come up with different proposal for 292
- 293 – Replace the title with Security Assurance Level assignment for …..
    - Agree with the subgroup proposal
- 314 – Refutation Objectives
    - Philippe – it is about what is required, not how we comply
    - Stefan - If you can achieve something through analysis, it is fine
    - Martin – new wording good, some things you cannot test, need complete coverage
    - Varun – why specify, if you do both, say you do both, up to applicant
    - Dave – haven't made specific recommendations, we are clarifying
    - Varun – test and analysis always done together
    - Dave – analysis in objective before
    - Philippe – does the note change the objectives?
    - No
    - Everyone agrees to change except Varun, he thinks it's redundant and not value added, but he is OK to move on
- 318 Section 4-2
    - This is about Requirement Objectives and higher-level design requirements
    - The basic resolution is okay option- The higher-level requirements with respect to the current level of security writing
    - Stefan S – Correct direction and needs some fine tuning
    - Phil W – Also in O3-6 needs to be changed to ensure consistent
    - The higher-level requirements are with respect to the level of requirements under development. Another option
    - John A/Martin C – should not be in glossary
    - John A – doesn't like the word level
    - Agree and close
- 319 Lower level requirements
    - John A. - Low level or lower level?
    - Stefan - Item level?
    - John A. – low level specific, those are the requirements at which you write code
    - Gilles D. – lower level, for security, must demonstrate in detail
    - Michel - Talk about aircraft, system, and item level
    - Stefan - Only for SAL 3 do we have to take it all the way down to code level
    - Armelle - 4.2.1 requirements section, no clear distinction between high and low-level requirements
    - Phil – term low level not used

        - Armelle – this section covers all levels of requirements
        - Michel – subgroup to revisit
    - 327 What are the mandatory standards
        - Stefan S – Mandatory from whom
        - Referring back to the editorial group
        - Stefan S would prefer to reject the comment and not to have the note
        - Stefan S –The existing note does not provide any value
        - Stefan S – Each applicant is expected to define coding and design standards need to define and justify the standards they need to apply
3. Adjourn for Lunch
    - 1214 Assets
        - Phil – already there, they changed asset to "logical or physical resource"
        - Dan – can just say protected from IUEI
        - Martin – agree, stick with terms in rest of document
        - Group revised and agreed to wording:
        - "…against intentional unauthorized electronic interaction…"
        - "…logical or physical resources…"
        - Phil – main point of comment was changing assets to logical and physical resources
        - Dave – don't like order
        - Dan – comment is vague
        - Phil reminded us no additional comments for this document
        - Dan - ARAC report – look at minor assets if they propagate to major (or higher) assets
        - Philippe – distinguish protection against IUEI and assets which are things that have major or above classification from safety point of view, objective of comment was to distinguish
        - As written, we don't have that
        - Dan – need to read whole section, this was a big discussion during ARAC
        - Michel – make first change with IUEI only, don't implement second wording change?
        - Move to moderated session again, too many opinions
        - Dan - Assets vs. logical and physical resources doesn't change anything
        - Philippe – disagree
        - Michel – sounds like we are starting another ARAC discussion which is not useful, either make first change only or go back to subgroup
        - Philippe and Gilles D. agree to Michel's proposal to only reword the first part – comment closed!
    - 1040 Assets
        - Cyrille is happy with the proposal – closed
    - 1043 Certification
        - Previously have agreed to remove so – comment closed
    - 395 Wrong Reference
        - Agreed and closed

- 1300 COTS
    - Subgroup sees no need for changes
    - Adrian is not available –
    - MM does not like the section too much, but does not have a big concern, so comment could be rejected
- 414 3-2-1
    - Consider replacing DAL with SAL or assurance level
    - Links to 158
    - Michel Not a good place to discuss this
    - Dan – could use high quality and low quality
    - Or high and low assurance
    - Just replace DAL with assurance
    - Philippe – does not believe this solves the comment
    - Dan the point here is assurance versus performance
    - Philippe – the text is talking about assurance and effectiveness, which is a source of confusion
    - Michel – the core principal is that there needs to be flexibility as there are different methods out there, and proposes to remove 28 to 36
    - Consensus to agree to remove
- 835 3-6-2
    - Subgroup proposes to delete the note and paragraph
    - Dan original process was – of you have a six-month patch cycle, but so many exceptions – so delete the vote
    - Alternative proposal – move the paragraph into the note and include "may take into account"
    - Agreement with the alternative proposal and closed
- 442 – 3-6-4 Misleading text
    - New proposal has been made and now need confirmation form Philippe
    - Agreed – and closed
- 444 – Risk Assessment
    - No objections to the proposal – accepted and closed
- 361 Use of COTS
    - Proposal was to remove the objective 7-2 and to reword 7-1
    - Gilles – There was a proposal from Patricia yes came out of the subgroup
    - Resolution accepted and is closed - Chuck is okay with this
- 865 4-1-2
    - Propose to modify the objective to include the test plans
    - MM Not convinced this is a good solution
    - Need to reword the objective or add a new objective
- 1165 Meaning of refutation
    - Proposal has been made by the subgroup, but is it sufficient to answer the comment
    - Clive to get clarification on what is missing
    -

- 1218 Refutation
    - Trying to clarify the 8-2
    - Phil would get away from analysis and don't use twice in a row
    - Michel – could try and come up with another proposal
    - Changed the sentence, agreement on the proposed change
- 1219 The objectives are unclear 8-6 again
    - Claudio - Include refutation test so that it isn't confused with standard testing
    - Moving onto comment, O1.2
    - Michel – Dan's proposal acceptable
    - Philippe - Did you check 326A? Should be in process document (he will look)
    - Ravi reading from 326A on the PASRA
    - Security development related activities
    - 3 people say pretty much the same thing
    - Michel – can we agree on another proposal?
    - Claudio – new solution is better
    - The need for security measures (deleting "to be developed")
    - Dan – resolve items or else we have a scope issue
    - Clive – from minutes, change security functions to security measures throughout
    - Martin – are we sure we want to do that at SAL 0? That means we don't do anything
    - Stefan – example is authenticity and integrity of load, put it on SAL 0, anything that has load would have to consider, that way don't need to modify standards
    - Which objectives do we want to go that far? Special objectives beyond security measure?
    - Phil – why SAL 0?
    - Dan - SAL 0 more dependent on security scope, what assets do we need to protect, applies to that scoping exercise, need to run our process
    - Phil – purpose of SAL 0 is that we don't have to do anything else
    - Chuck – other committees working this, in this document it shows as a general requirement on CM, to not even raise that as part of a report out seems to be dodging responsibility
    - Extends beyond committee to implement, raise as a point
    - Martin - Extending toward items security centric, not everything
    - Dave to Chuck – sounds like you (we) have an action to go to RTCA and EUROCAE and tell them they have a wider problem…and remove from document if you get concurrence that it's a bigger problem
- 460 Risk Assessment
    - Sub group proposes to modify the objective – change developed to implemented
    - Dan has a problem but will accept it
    - Modify to identify the need for security measures – alternative proposal

- Romauld – There is definition ARP4754 chapter 5-4
- Dan – is this now a discrepancy of level of requirements
- Referred back to 326A
- Security no different to other development processes
- Gilles support Dan – if we follow process, we talk about security objectives for security needs
- Ravi – 2-1.1 reads from that
- Romauld – objectives instead of measures?
- Final resolution agreed and closed

- 1220 Objective clarification required
  - Dassault should propose a text of the editorial group proposal is not clear enough
  - Stefan – In Europe could delete 4-1-5 as detailed requirements will come out for organisations under EASA audit, but FAA purposes we probably need to keep?
  - Michel – This is party of handover
  - Philippe wants an explanation – Stefan
  - No change to text ED203A scope is up to (S)TC while ED204 addresses the in-service phase
  - Comment is closed
- 1224 Objectives
  - O4-7 – Security functions - and use of functions ambiguous
  - Michel proposal from sub group is not understood
  - Dan – Didn't we agree to remove functions
  - See comment 462
- 363 Security Assurance
  - Subgroup proposes no change to the document
  - Propose an answer to this as a clarification for Chuck
  - Back to what assets we want to protect to determine the SAL 0
  - Chuck – wants to remove and raise the issue with RTCA/EUROCAE as out of scope.
  - Comment 363 -> same action for comment 376
  - **Action – describe out of scope aspect / issue to RTCA and EUROCAE, close comment**
- 1227 Discrepancy between the objective and the activities
  - Varun to John A. – why do you need to repeat QA objectives for security?
  - John A. – why do you need to repeat CM objectives for security?
  - Varun – built as part of system, software, design
  - Stefan – other companies felt the need to repeat objectives because there was the feeling that if you set objectives but don't state QA it might not happen
  - Varun - Don't want a separate review for the security part
  - Michel – look at resolution again
  - Gilles D. – subject is technical objective, don't know how to implement this
  - Gilles – would like to remove the objective

    - Back to the editorial group
- 509 4-4 The introduction is misleading,
    - Agrees to the first option
    - Resolution accepted - "A Security Assurance Level is assigned to security measures and assets* that have been identified in the security scope (see section 3.1) and risk assessment (see section 3.2) process activities"
    - And add a footnote to "assets" to detail that only SAL 0 is applied to assets.
- 894 Section on SAL should be moved
    - We have already moved it once
    - Martin – what is the common practice
    - Leave it as it is, and just refer to it in the introduction as its missing
- 895 Update guidance
    - Stefan will partially withdraw the comment
    - We need the text to do both
    - Proposed text was reviewed and made consistent
    - Do we have agreement to include the text – accepted
- 898 Update level of threat to consider SAL
    - This is already mentioned in 3-6-2-1
    - Propose to change the text in 4-4
    - Stefan does not believe it is clear but could live with it
    - Proposal agreed and close with the change
- 904 Use of COTS – in safety world this is only DAL D
    - Subgroup disagrees and think it's out of scope of the document
    - Stefan – it's not acceptable; for Hazardous. This came from we are using COTs security
    - Dan In COTS section – we have three classes – e.g. previously certified
    - Chuck philosophically has a problem with saying something has no DAL, and you are using that to mitigate something hazardous
    - Michel – Would agree to remove the proposal in the definition
    - Phil – Would it be sufficient – without access to source code,
    - Dave and Chuck – probably no
    - Dave – completely disagrees with the principal
    - Chuck – You are trying to introduce a concept of the introduction of commercial – and it has always been rejected
    - Philippe - Can we stick to the comment
    - Martin – So if the system we are discussing – then all assurance level requirements
    - Varun – COTS has been used for level C, you just need to know when it fails
    - Dave – excluding COTS and remove COTS, and disagrees with the way it is stated
    - Stefan – its products where we don't have access to source code
    - Proposed resolution – "access to source code and/or hardware description"
    - Dan – in section 2 – you need to look at what evidence you have and fix the delta

        - Martin – There are products we consider COTS and we apply to a platform – e.g. ARINC 653
        - Stefan - If you have something with a DAL certificate then it is not an issue
        - Resolution to delete the last two sentences –agreed and closed
    - 1094 The numbers
        - Proposal is not to change
        - We should explain why we don't have A to E
        - Varun – still considers it is an issue if they don't match up
        - Back to the subgroup for an explanation
    - 1319 IFEC may not be in a position to auto-assess level
        - Subgroup does not believe this should be included in this document
        - Agreed and closed
    - 554
        - Useful to provide such guidance, probably need to look at a future revision of this document
        - Commenter has agreed – so close
        - **Action item for a future activity that needs to be considered after document is published**
        -
    - 1320 SAL
        - Consider 'sufficient' this raises more problems that is solves, its moved to chapter 5 so no longer AMC
        - Comment closed no changes to the document
    - 912 Section 4-4-3
        - Provide actual considerations for decompositions
        - 4-4-3 is going to architectures as previously agreed
        - Agree with the deletion "Similar considerations to the end"
4. Michel – some NCs have been closed (via email)
5. *Adjourn*

5 Friday, March 23, 2018

1. Administrative Remarks – Michel M
    - Lighter attendance per usual
    - Progress – closed over half the NC comments
    - Again, only going to take detailed notes if a comment generated a lot of discussion
    - 596 - Risk acceptability
        - Suggested resolution is to delete the bullet
        - Dans concern was the word justify, and would accept alternative text
        - Level of threat reduction is associated with the security assurance for the security measures and other elements
        - Proposal accepted, and the comment is closed
    - 445 Risk Acceptance
        - New proposal was shown
        - Phil questioned whether this was expressed elsewhere
        - Stefan – is this better in 3-4-2

    - Stefan – Can we shorten this if we use section 3-4-2 which is threat scenario consistency and completeness and make the link there
    - Stefan – if it in appropriate not to include it here, but need to make it short and clear and more precise
    - Michel – Do we need the figure as it is only a simple case
    - Stefan – can we refer back to the editorial group and get them to wordsmith
    - Dan – if we agree the words as is, and if people want to wordsmith it later
    - Claudio – would like to have this proposal and analysed with the other text to see if it is acceptable
- 848 Security Assurance – re-arrange the objectives
    - There is a proposal that starts to do this and Michel went through it
    - John – Your adding activities and not objectives
    - Michel – in 4.2, referring to "augmented" and "regular" security development assurance objectives rather than supplemental and independent
    - John A. - Adding activities rather than objectives in first sentence of first bullet, you want assurance objectives
    - Michel - Activity from existing object
    - John A. - Activities are not normative, so we have an issue.
    - Dan - Augmentation considerations instead of supplement considerations. Augment is when you have to do that consideration and not think of it in terms of activities
    - John A. - Same problem as 178C, is activity required or something an applicant can use as info and plan on their own? Some need to be required and some not. Big problem with 178C
    - Martin – thinks it presents same meaning
    - Dave – to make Cyrille's job easier and have checklist, should be listed as objectives and not activities, some have verbs
    - Stefan - Objectives should not be activities, some critical enough to be written as objective
    - John Angermayer – activities that are important enough to be specifically required have been made into objectives in DO178C using "is satisfied"
    - Example – code coverage in 178
    - Michel – don't want to start reviewing objectives in tables again
    - Patricia – agree, try to make objective consistent for security, some in between security and safety, did not define pure safety and pure security because then there would be duplicate objectives
    - Dan – appendix that is normative only has objectives, we have room to do what we need to do between the different viewpoints, go ahead and deal with problems later
    - Michel – go through main proposal, last sentence added, difference between augmented in regular in Appendix A
    - Martin – change supplemental to augmented in other places?
    - Yes
    - Dan went through table and changed entries
    - Conclusions – agreement on the general direction – and this is not considered a non-concur anymore

- 462 Objective 4-7
    - No update from Antonio – should have an answer Tuesday
- 543 Security Coding Standards
    - Still waiting on feedback, feedback to date is probably okay but problems is showing compliance
    - Discussing Boeing NC coding standard comment from Don Heck
    - Stefan to Martin – what did your colleague say about resolution? Might be able to further refine text to address his concern
    - Need to give AR the right tools
    - Michel – another comment on coding standards, different text in document and high comment
    - Stefan - For 178, Boeing has a software coding standard pushed to suppliers to be used if they do not have their own, things will have to start now as suppliers have not thought of this – OEMs may provide "secure" coding standards for suppliers who have not generated a suitable one
    - Martin – yes, please add some wording on that and it will alleviate concerns, additional concerns but would knock down the non-concur
    - Conclusion solution is sufficient but not ideal solution and the comment was closed
- 1228
    - Skip to next one
- 367 SAL Allocation section
    - Skip as no new proposal, and we need a response from Chuck
- 896 Providing a relationship to DAL or Impact
    - Dave - Don't know how to resolve without equating SALs to DALs
    - To make augmented process work, need 5 levels with similar meaning
    - Martin – augmented means in addition to, so you are still doing safety prescribed by DAL, and then you are augmenting by adding SAL, not less, always more
    - Don't need one to one because you are always doing more for safety, never less
    - Minimums defined for threat condition
    - Stefan – equating SAL to severity, not in tabular format
    - Table shows how we design SALs, but doesn't talk about severity in any form
    - Text discusses rules, option to turn text into table, nothing is really missing
    - Dave willing to put forth a quick proposal
    - Sam – we worked on a proposal last week, need to email Michel a copy, show and modify it, at least we have a start
    - Phil – Michel is adding recommended edits to current resolution, problem with supplemental consideration sections, if we make these changes, make it clear
    - Proposed – comply with all objectives, high assurance
    - Removed all, added words to apply only ones you should apply, not easy to figure out in 3 weeks
    - Mitch – reminder that it took 10 years to go to 178B, same learning curve here, we can come up with something we can live with
    - Stefan – if we specify software, we need to specify hardware as well, not just working with software
    - Siobvan presented a mapping idea

- Oversimplified, no one liked it
- Michel – tried many different mappings, none worked
- Martin – before we give up on mapping, these are the minimums
- Phil has a mapping too
- Dave – if we use augmented method, need to be able to translate, need to map to existing activities, what is listed in these tables currently doesn't translate to DAL
- Dave presented a table different where it shows DAL to SAL (Siobvan's was SAL to DAL)
- Michel – might not find any such table
- Patricia – SAL 0 is minimum but can add security measures
- Steve – no problem with table but principles of 254 address how to go about doing it, not tabular form, but descriptive enough
- Martin – for Minor and NSE, would like to update to be clear, if no path to higher threat condition, fine
- If there is a path to a higher threat condition, will need to do more
- Dave – catastrophic better be the same rigor as safety, don't see that with the mappings
- Michel – this is a translation of assignment principles, no statement of certification or acceptance, no statement of assets and threat scenarios, should not be confused with protecting against threat and failure conditions
- Security deals with threat conditions
- Stefan – assignment does not modify DAL, this is about what I need from security perspective, mixing things up
- Martin – to Dave, don't understand your concerns, not replacing design assurance, safety still doing rigor per safety process, cover missing pieces for security
- SAL 3 + DAL A -> all the rigor you need for a catastrophic impact system
- Philippe – where are the connections? Most of the time, the connections are in low safety impact systems
- In all the example I know, the SAL 3 security measures will be implemented in level D systems
- Need to be developed properly
- Huge impact – don't want to introduce malware that could be on safety critical systems
- Dave – if security and safety assigned to same assurance, great
- What Philippe said would be my concern, a situation where a security measure protecting a catastrophic is implemented at a minor
- Look at how air framers develop their architecture
- Gilles D. – this table does not concern allocation and solution
- In Melbourne, I showed solution to implement and allocate SAL, ISAL (Item SAL)
- Can take benefits from safety assurance activities
- Voting on whether or not to include table
- Martin requesting text on path vs. no path so that someone doesn't misinterpret table

    - Dan – not method for determining what is in and out of security scope
    - Dave – Accepted for now, he still has issues on how to manage in practice
    - Committees agreed to include mapping table, close comment
- 897 – Ties in with 3-5-1
    - Concept and proposal to be shown, are people happy with the direction
    - Stefan went through the proposal, including inclusion of new examples and cleaning up the existing examples
    - Michel – Is this a change proposal for the document and where would we put it – 3-5-1
    - Michel disagrees to replace
    - Martin – keep the three first paragraphs and add the text
    - Remove the examples and tables and move to the Appendix I on architectures
    - Update the text and move the tables and examples to the appendix
    - If we call it common model for security – should it be kept separate from safety
    - Sam Stefan Dave, Martin and Dan to take forward as an approach
    - General approach agreed
    - Does this also deal with Dave's comment - Yes
- 1063 Errors in table – still need the feedback
- LUNCH
- EUROCAE TAC this week agreed to update the TOR
- Anna gave an overview of the updates, and happy to make a joint committee
- Michel WG-72 and 216 should ideally work closely
- Anna - down to a PMC decision
- Is it on the PMC agenda DO-204 and DO-355
- 1228 and 1316 Security Assurance
    - Back to comments, looking at section 4.2.8
    - Martin – Boeing test team has concern of TQL5, COTS test tools, it is not as simple as describing what it does and keeping a version to repeat a test
    - Still concern that might limit ability to use cert tools for test – don't want to do that
    - Is there an issue with qualifying these so-called hacker tools?
    - John A. - Look at what tools does, downstream verification; that determines whether or not you need verification
    - Varun – not every tool you use requires qualification, output thoroughly tested
    - Michel – we seem less concerned about first time, want to focus on that, maybe note that this section will not address all tool verification aspects, expand on it in future
    - Stefan – compiler produces something you test, you don't need to qualify compiler
    - Right amount of choosing tool and having that configuration control to repeat
    - DO-330 discusses objectives for COTS, very little for TQL5
    - If you buy off shelf, have even less
    - Varun – all examples are verification tools, easily check output, not a development tool
    - Martin – comes down to interpretation

    - Tools he is talking about are refutation tools, not verification tools
    - Lots of discussion
    - John A. referenced chapter 12 from 178C, remove TQLs as those are already in 178C
    - Stefan – if you don't find error that leads to vulnerability, then you won't find vulnerability, need to know tool limitations
    - Varun – this topic is in the weeds, we need to focus on closing NCs
    - **To be resolved together with 1228**
    - Looking at 1316 and security tool management objectives, NC from Philippe
    - Philippe - Don't want to shoot yourself in the foot with how we define requirements
    - Stefan – can merge 4.2.8 and 4.29
    - **Action to subgroup to rework O13.1**
    - Siobvan uploaded a couple rewrites to example methods for the group to review and concur that high and non-concur comments have been addressed
- Continue going through high comments
- 5.2 seems to redefine terms already in glossary
- Looked at comments metrics again
- If we have time, try to work out proposals for medium and low comments (otherwise reject?)
- Need to address all comments with priority on high and NC
- Michel will provid updated document before DC meeting week of April 9
- Dave – official plenary is closed
- Adjourn

6 Main decisions and actions

Decisions		

Actions	Who	When
Architecture – 5.6.2 Integrity of Data Loading - Rewording		
Architecture – Comment 300, 301, 302, 350 – Update definition		
Don't change 2.2.1, address in 3.3, discuss with commenter offline and resolve	Phil, Martin, Siobvan	
Review use of AEH	Stefan	

Example methods – discuss and close NCs and High Comments	Siobvan, Claudio, Dan	
IUEI - Discuss offline with people conflicting opinions and come up with rewording	Gilles	
Risk acceptability – side conversations needed		
573 - Review musts and should in document		
1216 - Discuss offline and come up with proposal for 3.5 high comments	Gilles	
Be explicit and move sentence to 5.6.1 for additional information for defense-in-depth	Siobvan /Michel	
897 - Work on proposal for common mode method for security relations	Stefan, Dan, Sam, Dave, Michel	
848 – Work on wording of objective	Stefan, Philippe	
375/376 - Wording of columns		
613 – Work out another proposal	Phil, Mitch, Cyrille Rosay	
1206 – Make changes discussed, putting 4.4.3 into 5.3.1 and appropriate references to 5.6.1	Siobvan	
New proposal for 292	SAL group	
363 - Describe out of scope aspect		
554 – Action item for future activity		
1228/1316 – Rework O13.1		

/s/
Siobvan Nyikos
Secretary, SC-216

/s/
Clive Goodchild
Secretary, WG-72

CERTIFIED as a true and accurate summary of the meeting