EUR 306-17/WG-72-105
RTCA 304-17/SC216-077 St Denis and Washington, 11 December 2017

Summary of the Meeting of RTCA Special Committee 216 (Meeting 36)
EUROCAE Working Group 72 (Meeting 48)
Aeronautical Systems Security

DATE: Nov 13th to 17th, 2017

PLACE: EASA, EUROCONTROL, Brussels

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

ATTENDEES:

			Nov 2017				
Name	**First Name**	**Company**	**13**	**14**	**15**	**16**	**17**
Alparslan	Hannes	EDA					M
Blaize	Raphael	Airbus			T		
Call	Martin	Boeing	T	T	T	T	
Cyprien	Cedric	Airbus	T	T	T	T	T
Flores	John	FAA		T	T	T	
Freitas	Joacy	ANAC	T				
Fuilla	Patricia	Apsys for Airbus	T	T	T	T	T
Gauthé	Armelle	Apsys for Airbus	M	M	M	M	M
Gobbo	Giles	Airbus	M	M	M	M	M
Goodchild	Clive	BAE Systems	T		M	M	M
Grant	Christopher	UTC	T	T	T	T	
Hannert	Larry	LCH	T	T	T	T	
Haury	Christian	Safran	M	M	M	M	M
Hofmann	Karan	RTCA	M	M	M	M	
Kelly	Mark	Esterline	T	T	T	T	T
Khanna	Varun	FAA	M	M	M	M	M
Kocsis	Mathew	Gogo.inc	M	M	M	M	M
Lamont	Kristof	Eurocontrol					M
Marchand	Cyril	Thales	M	M	M	M	M
Marquis	Philippe	Dassault Aviation	M	M	M	M	M
Messerschmidt	Michel	Airbus	M	M	M	M	M
Moreaux	Jean-Paul	EASA				M	
Morrissey	Patrick	Rockwell Collins	M	M	M	M	

Nagel	Benjamin	F-Secure	M	M	M	M	M
Nori	Ravi	Teledyne Controls	M	M	M	M	
Nyikos	Siobvan	Boeing Commercial Airplanes	M	M	M	M	
Pierce	Dave	GE	T	T	T	T	
Rosay	Cyrille	EASA	M	M		T	
Royalty	Chuck	Aerospace Systems Cyber Security	T	T		T	T
Salgues	Romuald	Airbus	M	M	M	M	M
Schwindt	Stephan	GE	M	M	M	M	M
Tinney	Tim	Saab Group	T	T	T	T	
Trope	Mitchell	Garmin	M	M	M	M	M
Waheed	Mohammed	Aviage systems	T	T	T	T	
Waller	Adrian	Thales	M	M	M	M	
Watson	Philip	Panasonic Avionics Corporation	M	M	M	M	M

M meeting, T telephone

1. Monday, November 13, 2017 Day One

Notes
Varun read Designated Federal Officer Statement
Karan – RTCA remarks

- Siobvan acting chair for SC-216 onsite
- Stefan acting chair for WG-72
- Showed RTCA committee membership policy and Proprietary Policy

Michel showed IPR policy call for EUROCAE WG-72
Agenda review
Dave – before editorial subgroups, need clear expectations of what we want achieve this week
Stefan – presentations from each editorial group, what changes proposed, what direction, identify where groups work together, must address non-concur comments
Just short 1000 comments in total! What direction will this document take?
By end of this week, review non-concur and resolve (or identify how to resolve) comments
Siobvan – showed minutes, don't need to go through them, main takeaway is that we were not ready for FRAC/Open Consultation and broke into editorial groups to resolve comments
Stefan – we want to go into December meeting expecting to be able to go to FRAC/Open Consultation and only need to resolve wording or minor things / have a plan for resolution
Don't want surprises
Michel – if anyone has corrections for minutes, please let us know, otherwise they are approved, minutes available on workspace
Michel showed the spreadsheet with the comments metrics
SAL and security assurance have the most non-concurs, a lot of time dedicated to those topics
Stefan - Redundancy in these comments, what paths can we agree on?
Skip action item review, action items superseded by comment resolution
Document Scope (Stefan, Larry)
13 comments, no non-concurs, closed comments TBD
Summary of changes

- Reword intro to be similar to ARP 4754
- Remove references to part 21
- Improve wording

Need for standards to cover this with upcoming EASA horizontal rule, but this may not be the standard to do this in
Topics that require discussion

- Overlap with other standards
- Requirements vs. process
- See ASTM F44

Peter Skaves comments via emails, we seem to be duplicating what is done in other standards, ASTM F44 does a better job of addressing just security, would like to see "process requirements"
Do we have a problem here? Need input from committee
Michel – don't have room to change document in another direction, might have opportunity in another revision
Cyril – process in ED-202
Stefan – are there technical requirements in this document? Doesn't seem to be, shouldn't be a problem
Varun – there are objectives, but how you meet it is up to you
Stefan – defer to SAL group, supplemental vs. independent approach, balance
Define what is needed for security

Chapter 4 – best way to achieve this, how to organize
Seems like everyone is happy with scope
Michel – can we make F44 available to the group?
Need to be part of that subgroup, hard to determine if we are OK without seeing what F44 says
Defer to chapter 4 and consider this comment closed
Phil – add note that this was against 3.1.1, as a result of many comments against 3.1.1, will delete several figures
Watch list – can't resolve until we see where document is going / comments are better understood
Future revisions will work on objectives – is that OK with PMC and RTCA?
Karan – cannot include any reference to future work/revision in document; give watch items for years out and any recommendations to PMC during presentation of document approval and publication
Stefan - If we achieved everything already, we can take out sentence, "A future revision of this document is planned to address…"
Karan – can also outline it in the TOR if the group desires to not sunset committee and knows there will be a possible revision shorter term (say, 2 years or less)
Be careful not to be too open-ended

Document Structure (Michel)

Don't have a presentation, so checking comment sheet
One non-concur from Dan – multiple sections with redundant content that is inconsistent with similar connect in other sections. See individual high comments
Has not received feedback from Dan yet, not sure what to do to make document more mature (aside from what we are already doing in editorial groups)
Stefan – question to Dave, can we close this non-concur?
Dave – if editorial groups resolve comments, document will become mature by next meeting
Michel – we should email Dan again on this one, attempt to close this comment
Order of appendices is confusing to reader (medium comment)
Appendices will be reordered - Normative appendices will come first
Not using an annex
Chuck proposed we (re-) define security
Michel – disagree, security already defined in documents and glossary, more general
Can introduce "airworthiness security" in glossary
Stefan – usually people read scope over glossary/definitions, so important to include in scope
Include image that defines aviation security, airworthiness security, and scopes?
As long as we are talking between editorial subgroups, there should be some consistency, some comments cover more than one topic
For example, level of threat should talk to combined protections and architecture subgroups

IEUI (Patrick, Cyrille M.)

IEUI = Intentional Unauthorized Electronic Interaction
7 comments, no non-concurs, all 7 in "proposal" state
Whitepaper on proposed resolutions, still need feedback from commenters
"A person compromising a system by unintentionally reducing or deactivating security controls." – wording from ARAC report, typo?
Stefan – stupid mistakes / accidents can lead to someone else being able to access something
Safety people only look at accidents
Patrick – look at misuse case of someone accidently misconfiguring a security function, would we address that in guidance material?
Michel – even isn't just disabling a control, it's also someone taking advantage
Rewording might be needed
Cyrille M. – they should be training and should follow procedures
Patrick – places where we are required to include operator guidance
Change unintentional to intentional because the attack on the system is a IEUI event whereas the

accidental misconfiguration is not the IEUI event
Reworded sentence, kept unintentional, but specified that the unintentional action enables an attack that would constitute an IEUI on system
Michel – biggest difference between safety and security, security deals with direct, intentional events
Siobvan – have not heard from Dan Johnson re: his action, topic of discussion for Architecture
Dan might need to designate someone in his place to complete document actions
Lunch
Architecture (Siobvan)
21 comments, no non-concurs
5.3 might go away
5.5 – physical security is out of scope for these documents though it should be a consideration / architect should state it in his/her assumptions
Martin disagreed as physical security is a big consideration
Around the room, physical security not part of the TOR so it is not in the scope, don't want to talk about securing cockpit doors in these documents, it is OK to get credit for physical security even though it is not in scope for this document
Resolution – add to the end "as it relates to protection against IEUI." (recorded in spreadsheet)
Also add "The physical security protections are typically considered in the security environment definition of trusted zones and access."
Also cover in section 3, security environment and trust
Check 3.1.3 for that information (Patrick)
5.9.3 – Martin wanted to clarify verification and validation should be treated differently
Does refutation belong strictly with validation?
Resolution – Change Title to Verification/Validation/Refutation to make everyone happy
Went into discussion of whether 5.9.3 (or 5.9 for that matter) belongs under architecture, should it go into an appendix or be covered by another section? Keep as is
Editorial comment throughout – need to be careful of words like should, shall, must, etc.
Need to it make it clear this is guidance and not requirements
In Europe, "should" might be interpreted as a requirement
Siobvan has action to go through words and make changes where something might be mistaken for an actual requirement, chapter 5 to start with, might help in other areas later
Topics of discussion
Security barriers vs. security measures
Siobvan and Michel had a side bar on this during break and determined it is OK to have security barriers as long as it is well defined in glossary and/or document
Siobvan – not in DO-326A, but shouldn't be a show stopper, whether or not we include security barrier does not change how we do security assessment
Patrick – should this be an editorial comment where we keep security barrier but review document for consistency of meaning
Siobvan to take action to look at both security barrier and defense in depth. Decide on one term. Make sure we are consistent in how we use the decided term
Next topic of discussion - 5.3 comments and whether we should delete 5.3 altogether
Dan had action to decide if anything needed to be moved into other sections and 5.3 deleted
Philippe brought up item vs. sub-item and how it relates to assurance
Resolution – propose we delete 5.3 and decide on definitions to add for assurance later (Michel)
Philippe – be precise when we assign DAL and SAL to an item
Stefan – need to check with assurance group on how to handle
Michel – move definitions from 5.2 to glossary
Siobvan – have in both places? Or delete 5.2 after definitions put in glossary
Some terms only used in chapter 5
Will revisit after assurance discussion this week

Combined Protection
No presentation, looked at excel file
No non-concurs
Need agreement on independence vs. diversity vs. isolation
Move definitions to section 3.5 on security measure characterization
Combined protection subgroup will provide definitions
Security Scope?
Clive can't make it until Wednesday, suggest shuffling topics to do security scope on Wednesday
Michel will show slides to prep us, but we will wait until Wednesday to discuss as there are 3 non-concurs for this topic
Phil – high level comment, how much have the groups been going back to the original commenters for feedback, is it supposed to happen already?
Stefan – depends, would have been nice to have been done before
Depends on progress, severity of comment
Certification (Stefan, Siobvan Cyril)
39 comments, 1 non-concur
Section 2.2

- Clarification to prevent misinterpretations
- Added questions for identifying protection and impact

Section 2.3

- Replaced major/minor (as related to changes) with certification since major/minor can mean different things to different people or depending on context
- Change vs. analysis of change
- Updated responsibilities of STC – achieve security as TC
- Removed levels to avoid confusion of DAL and SAL

Section 2.4

- Clarify operation and aircraft guidance

Topics that require discussion
When STC makes mods to connect to aircraft system without OEM data packages
"Bi-directional security" – is it possible?
Secure STC from aircraft as well as aircraft from STC
Varun – overloaded terms, don't want to use in this document
Romuald wrote working paper on this topic, don't need example
Should go with text of ARAC, don't revisit
Siobvan – want to make sure that the STC holder has a compelling case if they don't obtain support or data from OEM, i.e. can prove that their system does not touch anything that would trigger special conditions or have security impact
They need to be held to same standards as everyone else, but I understand there should be balance
Keep text with minor edits, revisit later
Stefan - "Level of security" – what are we talking about? DAL or SAL? The suggested security architecture
Need to determine which one
Michel – "amount of security"?
Resolution – delete paragraph, this is discussed elsewhere
Next topic of discussion – asset protection, which systems need to be protected?
Minor and no safety effect systems
Need to coordinate with asset subgroup
Martin's non-concur comment – It does not matter what the change is, the aircraft security level assessment is always required…This is a particular problem for STC where applicants contend to only

address the new/modified system
If you move it somewhere else and cover it, we are OK
STC applicant must comply with special conditions and CRI
Should be covered in document under what an STC holder must do (Stefan and Michel)
2.4 note edited – If an applicant has to produce aircraft level certification evidence, the certification evidence includes but does not need to reproduce the system level certification evidence.

Continued Airworthiness (Varun, Dave)

Varun – operators like how DO-355 is written
Need feedback from Martin and Stefan on comment resolution, go through comments now
New text provided for section 2.5
Martin's comment OBE with new text

Risk Assessment (Philippe)

37 comments, no non-concurs
Discussed whether we should delete core principle #2 from 3.2.1, "Existing safety processes have not had to consider intentional disruption, which is the focus of airworthiness security."
Make it a note to core principle #1 rather than its own principle?
Patrick – should already know this if you're reading the document
Michel – there were more comments on whether or not we even need these core principles
Siobvan & Varun want to keep principles, true and important
Siobvan – counter argument is that these principles should be earlier in document rather than deleted, my management wants these in the document as well
Resolution - Move text from core principle #2 to 1.2 Scope
Discussing comment #269 and purpose of document
Patrick wrote this suggested resolution as cautionary text
Stefan – we already have text in there
Martin – applicants and regulators decide on MOC, then everyone who supports them must follow that MOC
Stefan – already have a sentence to the effect of if you already have an established process, you can follow it
Patrick – we are trying to provide guidance to companies who don't know what they are doing
Few people who know both cybersecurity and aviation
Michel – many methods in document
Patrick – this resolution is not redundant because of the way the purpose is wording, talks about future rather than existing, my reference is to existing
Stefan – you can have your own methods, but you need to prove that they work
Michel added text from ARP 254, deleted all but first sentence of purpose
Adjourn

2. Tuesday, November 14, 2017 Day Two

Risk Acceptability (Philippe)
19 comments, no non-concurs
Looking at risk acceptability tables
Philippe suggests keeping both tables so both points of view can be considered

- Table 2-3 is more of a safety point of view
- Table 2-4 is more of a security point of view

Martin – still have a problem with table 2-3, minor and very high being acceptable, even though that came out of the ARAC committee
Philippe will address when we get to that comment
Proposal from Dave was to delete 2-3 and keep 2-4, several agree
Dave – one table was best for evaluating situation, the other one was superfluous, the "3D table" gave us the full picture where the other one didn't
Stefan – thick line (in another table/chart) indicates there is room for negotiation, thin line means you either have acceptable risk or you don't
Safety has continuous numerical scale
Larry – I don't understand argument that you have historical quantitative safety, in safety doc many aspects are incalculable and qualitative in nature, why are you saying security doesn't have same issue?
Martin – tables are redundant but no harm in keeping both if different people like different tables
Cyril – some activities are not 100%, look at gap and say OK or not OK
Romuald – need more flexibility
Resolution – remove table 2-3, will need to change text slightly
Reworded paragraph that starts, "Consequently risk acceptance is based on a two-dimensional assessment…" per Siobvan comment, clarifying terms
Need to mention all methods and their corresponding appendices, now up to 4 methods proposed by Airbus, Honeywell, Embraer, and Boeing
Currently, only references 2 of the 4, need to correct
Philippe – in table 2-4, we don't consider minor and lower systems
Those are addressed in section 2.2.3
Stefan - Need to address why Very High Minor is Acceptable, per Martin's comment, use a * in the table
Martin – Acceptable implies you don't need to do anything more, yet you need to assign SAL 1 to everything, contradiction, if a system has minor or no safety threat condition but there is an external access point, you need some security measure implemented to protect the aircraft
Don't want people misinterpreting this and designing systems with vulnerabilities
Philippe - If system provides access, it will be in a threat scenario
Martin – majority of people will be looking at this from a safety perspective
Chuck – security and safety have to match, applicant can do more but that isn't required
Martin – if there are a lot of threat scenarios that involve that minor system, there needs to be security measures
Patrick – it's a design choice
Martin – it's also about certification
Don't want to assign SAL to systems that don't need SAL
Michel – don't make assumptions yet, we will revisit this tomorrow during SAL discussion
Looking at section 2.7.1
Philippe – agree with Stefan, risk acceptance should be determined per threat condition, not threat scenario as text currently says
Martin – acceptable the way it is written

Philippe – could be a source of confusion
Michel - Risk is combination of level of threat and threat condition, now we define scenario to be evaluation of level of threat for threat condition
Philippe - Risk defined by threat condition, afterwards you identify all threat scenarios associated with threat conditions
Stefan – In safety, failure condition can have one to multiple ways of being realized, i.e. scenarios. Should be same for security
Michel - Never defined risk of threat condition, only of threat scenario

Assets (Cyrille M.)

Sub-lists were not complete and misleading so they have been removed
Ensure we use the same definition of assets, just say asset (rather than primary asset) and use definition from glossary (no change)
Consider logical and physical assets
Minor and no safety effect systems – may become asset if assessment determines it impacts airworthiness
Romuald – Need security measures to prevent propagation of threat
Michel - Security measures are assets
Replaced "asset" with "system" in several places
Reviewing comment that spans both certification and assets
Bullets in question:

- Are security measures implemented in the system required for layered defense?
- Is the system an electronic access point…?

Martin suggests we add those bullets to 2.2
Michel – this should be captured by new statement about requiring protection for their own sake
Stefan – no, doesn't cover security measures
Cyrille M. - Here we introduce layered defense, might cause confusion
Siobvan - Layered defense or defense in depth not discussed until chapter 5
Michel - Security measures discussed in 3.5
Martin – for fluidity of document, you need to have discussions here
Phil - Are 2.2.1 bullets covered by ones in 2.2?
Martin – second one is but not rest
What is purpose of introducing?
Martin - Bring to light minor and no safety effect systems provide access which leads to vulnerabilities if you don't add protection
Michel – confusing to talk about security measures in this section
Martin – starting to see Michel's point, defense in depth bullet can be covered somewhere else
Phil – look at later sections on defense in depth and decide if they address your concern or if more is needed
2.2.3 has changes similar to 2.2.1 and 2.2.2, consistency
3.1.1 – asset identification, removed all the examples
Lunch

Logging (Phil)

12 comments, 1 non-concur
Removed CONOPS #7 due to objection airworthiness at a minimum, already covered by CONOPS #6
Martin – this leaves it up to the DAH to determine what should be logged, are the regulators OK with that, Varun and Cyril?
Varun – Agree, STC holder might need to log too
Martin - Not just airworthiness, point of security logs is to figure out what is going on, get evidence to address problem, logging is for 1) evidence chains and 2) proactive interaction
The con to leaving it to the DAH is that you might get a wide range and some of it might not be useful
Shouldn't it be in the regulator camp?

Romuald – regulator mandates ability to log, after that, it's up to the DAH
Crew alerting different from logging
Special conditions – Martin got the impression FAA and EASA wanted logs for different reasons
Patrick - Are you referring to AC 119?
Martin – it's in there, but I'm referring to special conditions
Varun, Dave, and others – regulators don't know your system, so how can they tell you what to log?
Log for unauthorized access or security rules that are tripped
Dave – special conditions are older now, might not be appropriate anymore
Michel – it is in special conditions / issue papers, but it's generic
Martin – what if an applicant decides they don't need to log anything
Varun read off logging from external issue paper
Romuald brought up negotiating the logging issue paper item
Varun agreed, depends on applicant
Michel – for example, we aren't going to do anti-virus
Romuald wrote the original working paper, the point was to give objectives and not be prescriptive
Special conditions in place until we have a rule, then there needs to be an AC to go with the rule
Resolution – keep as up to the DAH
Phil – a lot of comments with 6.1.1
Flight crew alerting – we shouldn't be doing that, where did that come from?
Title is still security notifications
Varun would do a non-concur if it was called flight crew alerting
Concern that pilots would have to look at logs or new flight crew alerts – not so
Alerts for safety already built in
Michel – to address non-concur comment from ALPA, perhaps we should delete paragraph in question
Dave - Methods and considerations document needs to provide guidance to the DAH, not meant to provide something new in flight crew alerting
Romuald – don't want to increase flight crew workload
Varun disagrees with Martin on letting the pilot know of a security event
"We are not fighting ghosts"
Don't want to gold-plate document and account for all corner cases
Michel – we should leave this out of document and if the need arises later, address it then
All agree
Delete sentence in paragraph about flight crew alerts
Security events that cause a safety effect could result in existing flight crew alerting following the guidance provided by AC 25.1322-1 and other documents.
Delete last paragraph
Patrick - Notifications was for the sole purpose of maintenance messages
Question – do we ever refer to an AC in an RTCA document?
Talking specifically about AC 119-1
Karan – we have called out other documents/references in other RTCA documents
Stefan - AC is technically not regulation
Varun – this guidance document might have a longer life than an AC
Last comment – quick reference handbook (QRH) concern from ALPA

Security Assurance (Armelle)

211 comments, 9 non-concurs!
18 closed
Topics that require discussion
Too many objectives and activities, need clarification
Stefan – regarding this, how is it different from other standards with objectives and activities? Not requirements
Proposal to simplify chapter 4

- Security specific sections first
- Activities moved into informative appendix
- Appendix D restructure
- Objectives reduced (by how much, we don't know, depends on how you count)

Dave – won't be easy for others to pick through these tables
Michel – looks different depending on what you are developing
Dave – trying to make existing safety process cover a lot of this
The reason for having SAL – if you have a DAL D device that has additional security assurance
Perceived complexity lower than it was in the past
Each subject has security development assurance objectives
Going through objectives tables
Dave showed his document to attempt to clarify
People need to meet airworthiness process whether by objectives or otherwise
Martin requested we end on time and pick this up again tomorrow afternoon
Dave at least wants to discuss what it should look like.
Adjourn

3. Wednesday, November 15, 2017 Day Three

Level of Threat (Cedric)
Looked at figure that shows relationship between effectiveness and likelihood
Stefan - 60 comments on this topic, what are the other changes, that might influence how we do the structure and diagram
Adrian – introduction was confusing, didn't say what it actually covered, now says what to cover as a minimum for level of threat
Patrick - Assurance is helpful in preventing bypass and other design flaws, doesn't relate to how well it defends against attacker
Is assurance defined wrong here?
Stefan - Does it do what security needs?
Adrian – two parts - Does it prevent attack? And have you implemented it correctly
Stefan - Assurance is am I developing the right thing and has it been developed correctly, SAL objectives don't cover if it is effective against attack, have we developed the SAL objectives wrong
Varun agrees
SAL needs to address security, otherwise we have done the wrong thing
Martin – assurance verifies development and design is what you expected, but also includes validation, do I have right security measure and is it sufficient, if we do assurance properly, it should also verify and validate
Stefan - If we are cutting out too many objective to be compatible with other standards, we might not get what we are asking for
Adrian – do we still have objectives about level of threat validation?
DAL relates to severity of effect - Do we do the same for SAL?
Need to edit SAL before editing text for Level of Threat sections
Put in the comments that we need to revisit this after we have worked out SAL
Moving some of the text into 3.5
Figure 3-17 should stay here, combined protection evaluation principle
Michel – one non-concur, level of threat but against appendix rather than main section
Martin – once we straighten out formative sections, informative (appendices) need to be revised too
Specifically looking at ED-202 (Airbus) method
Dave – tried to work through examples and numbers could be used inappropriately, need to be justified by applicants, considerations in method and applicants justify numbers
Engineering judgment is how you get the numbers
Numbers might not be appropriate
Is method sound? Does it give results that are repeatable? If not, that drives a non-concur. Don't know how to fix it other than have applicants justify their numbers and scales
Michel - Same comments would apply to likelihood method and other methods, concerned about a non-concurs, makes document impossible to apply, haven't found method that is good for other organizations
Stefan - Numerical scales will always be subjective, look at ISO, this is why it is important to define objectives
Philippe - Security – need to provide evidence, safety follows different process
Stefan - Safety – need to prove it's effective
Siobvan – while I did not put a non-concur against this method, my comments echoed Dave's concerns. In addition, how I thought this should be scored was different from how it was actually scored, perhaps I should walk through method with Michel or someone else familiar with method and help to add clarifications where needed and clear up non-concurs
Dave will look at responses to comments during a lunch or break
Varun - If appendix material is misleading, can cause an issue, that would drive a non-concur only in that

aspect. If I don't like the method, that's not enough for a non-concur
Michel – also a non-concur against appendix C, Dan not available, who can address?
Ravi volunteered to address non-concur against appendix C likelihood method

Trustworthiness (Raphael)

No presentation, going through comments sheet
Proposition to move some text to security guidance part of assurance
Physical access – trust assumptions may include but are not limited to the following external entities

- Saying no causes problems in Europe
- Saying yes causes problems in US
- Say "may"

Paragraph that implies legal and social means by which public can be trusted, not the case, a couple comments on this, edited to clarify
Stefan - Social means or norms are not a robust protection
Phil – the thought behind this is that if a passenger is physically messing with the IFE, another passenger will say something
Michel brought up smoking in lavatory example
Martin – no one has ever checked my laptop at the airport for hacking tools, they only look for physical security not cybersecurity
New text - Passengers are and non-traveling public and their devices are generally assumed to be untrusted entities for the purpose of security risk assessments.
Can trust passengers in private jet…if you feel like it
Different set of rules, for example, don't need cockpit door on private jet as the owner of the airplane is not likely to take out their own pilot

Security Scope (Clive)

38 comments, 3 non-concur
Non-concurs around Figure 1 as well as STMPA-SEC method – fixed to address Chuck's comments
Phil - Aren't these the same figures the asset group decided to delete?
Yes, no issue with removal from editorial group
Need to simplify sections and remove misleading bullets to address a lot of these comments
3.1.5 Decomposition of Assets to be moved into chapter 5 architecture – action to Siobvan

COTS

EIA standard
Discusses anti-counterfeit management plan – Stefan sent what he is reading off for additional info (see below)
EIA-STD-4889-C is now a SAE document. If you reference EIA-STD-4889-C (used only by Boeing) then you also need to reference IEC TS 62239-1 (used by Airbus, COMAC, Embraer and the rest of the world) as both are ECMP standards and both address anti-counterfeit management (clause 3.3.2 in 4899 and 4.3.9 in 62239-1) which refer to SAE AS5553 and IEC TS 62668-1 (and -2) which asks the OEM to write and comply with an anti-counterfeit management plan.

These anti-counterfeit management plans ask for the OEM to conduct mitigation testing when buying any untraceable components or investigating unusual failures which might be previously undetected counterfeit or fraudulent components. The OEM can use the SAE AS6171 suite of 19 anti-counterfeit mitigation tests. Unfortunately SAE AS6171 is very expensive to use in its entirety and users will typically 'cherry pick' what they think is appropriate depending on risk. Also SAE AS6171 is trying to establish a qualified Third Party test house list which could be considered a barrier to international free trade as only the USA might control this. One of the newer test methods ***still in draft*** *is AS6171/16 ' Techniques for suspect/counterfeit EEE parts detection by Netlist Assurance Test methods', see attached which is targeted at trying to find out if a microcircuit has been tampered with. Of course a good part is needed which has been previously analyzed by SAE 6171/11 ' Design recovery' as a reference which might lead to complications on die revision history*

or manufacturer undocumented die changes as it is assumed that an independent Third Party Test House will conduct this testing. Personally I think this will only be valid if the original manufacturer does this testing as only they will know the exact configuration of the die. This method will be cross referenced into the next revision of IEC TS 62668-2 which is referred to in both ECMP standards.
Stefan - We want people to have an Electronic Component Management Plan (ECMP), but don't want people to go down rabbit holes
Michel – just state that you should have an ECMP, don't need to spend a lot of time or text on this
Should we refer to one or two standards as examples? Might be too difficult
How to keep yourself current?
Recommend remove standards and state things expected in ECMP, Stefan has action to provide wording and what is expected
Responded to non-concur
How to define exhaustive testing? Could use SAL 2 to describe extend of testing
Varun - How you define it. 254 says all inputs and outputs have been exercised once
Protective function vs. final function is a consideration
Added "Security testing should provide confidence on product behavior…", linked to objectives from chapter 4
Discussed Siobvan's comment #480
"Applicants proposing to use legacy systems for airworthiness in general are to perform a change impact analysis based on the proposed intended use of the function and how that intended use differs from the original use of the function." - when would someone use a legacy system for something different than intended? I would be more interested in how it is integrated
Sparked more conversations / issues
Varun – what should you being doing for an STC on a legacy system?
Patrick – Stefan, are you trying to formalize something that is typically done informally?
Siobvan – "change impact analysis" might not necessarily be something formal turned into authorities, might be something done informally and internally to determine if there is cert work
Stefan – part numbers changes are major changes, even if all you changed is color, under EASA rules
FAA rules are different
Gilles - Possible to do activity but not required for certification
Change to: Applicants proposing to use legacy systems for airworthiness in general should determine if there is a security impact based on how that legacy system is integrated and impacts the interfacing systems and overall airplane.
Stefan - We specify this in 2.2 and 2.3, what to do for airworthiness security
Added reference to 2.3
Stefan – in 202A we originally called out CIA for all changes
Patrick – what was it driven by?
Stefan – don't know, wasn't involved at the time
Varun – state what you are doing in the cert plan
Patrick – see Stefan's points, but want to be careful of wording, especially if the regulatory is saying they need to be careful
Michel – let's not talk about 202A and 326A right now, not planned for revision at this time
Varun – CIA came from software, can be a big thing
2.2 has content of FAA policy statement
2.3 has design changes
No agreement. Action Romuald to propose another resolution
Lunch
Security Assurance
Varun - Don't duplicate objectives from software and repackage them as security, think of auditing
Stefan - How do resolve when DAL is different from SAL? For security parts, what is common to 178? What is different / security specific

Until we know proposals, hard to address
Varun & Dave:
General case – outline what needs to be done from 178, 254, will cover 90% of objectives
Special case requires additional work, and that is what you need to specify
Patricia – proposal currently in document was approved by Dan, he agreed on combined
Michel - Now we are raising the complexity, some apply in some situation and not in others, challenging to describe
Philippe - We don't have an agreement of what is required for SAL 1, 2, and 3, need that before we decide on how to present all this
Varun agrees, and has raised this before
DALs determine amount of errors and amount of work done to prevent those errors
For security, it's the protection layer on the function, make sure you have adequate rigor for function for level it is associated with
Clive – work on one problem at a time
Varun – need to look at SAL definitions
Michel – Dave's proposal yesterday is maybe we don't need a SAL at all
Do we want to define SAL now? Or not use it?
Stefan – if there were not processes, safety or otherwise, what would we want to do for security
Avoid double auditing of activities
Ravi – all that work was done in the summer, now we are circling back
Stefan – a lot of it is presentation, don't want applicant to think there's a bunch of work
Dave doesn't want to force anyone to use SAL
Doesn't necessary work with / applicable to all architectures
Patrick – good to have developers of level D and E systems consider security without having to raise their DAL
Dave – Level E shouldn't allow propagation. If a level D system allows propagation, it should be higher
Martin – not true, correctly there are level D and E systems that provide access points and allow propagation, all they care about is that the system doesn't catch on fire
Brought up dataloaders
Michel - If you follow failure conditions of 178, you don't need to consider intentional. That is what we are trying to do here.
ATN over IPS – just applying DAL is not enough, other standards not prepared to handle security
Dave wants chapter 4 to be the norm, easy to follow, 80% solution
Discussions came full circle and back to defining SAL
Reviewing SAL map spreadsheet
Dave – problem is people think the supplemental approach should have a smaller number of objectives
Varun – if it's unique, we need to do it, just leverage as much as we can with what we have already
Looking at SAL definitions proposed by editorial group, no agreement within editorial group yet
Michel level setting
We agree that we need a minimum SAL
Before we assign a number, is the minimum different from the SAL 1 describe here?
Yes because SAL 1 implies some activities
Can call minimum SAL 0 or renumber 1 through 4
Decision: SAL 0 through 3 where no work is required for SAL 0
Full definitions will be in notes for comment #744, can include in notes after they are decided
Adjourn – Team Dinner

4. Thursday, November 16, 2017 Day Four

Security Measures (Stefan)
17 comments, no non-concur
Several comments don't have a proposal and it is unclear what the commenter wants
Is SAL characteristic of security measure or output of design process with required level of determined by level of threat activities?
Discussing Chuck's comment
Martin - Part of SAL assurance is requirements validation, is it the right requirement, is the security measure going to be implemented, isn't that what it is?
Ravi – clarification – are we tying SAL to DAL? No
Stefan - Is SAL a characteristic of the security measure? Or a characteristic of the design process? Need to decide and write it in document
Ravi - If you are tying SAL to level of threat, then you are tying it to safety? Which is it?
Stefan - Need to do SAL assignment first before we can answer that, tied to safety but not tied to safety in the sense of DAL
Philippe - SAL is determined by two things

- Strength of measure
- Level of confidence

Prefer level of confidence considered when you determine level of threat
Ravi - Desire to create cookbook for risk assessment is a waste of time, determined by problem you are trying to solve, won't know things until
Philippe - Time input, activities follow a certain sequence, level of confidence part can show up sooner or later, take existing measures into consideration
Ravi - We don't have luxury of designing from scratch, older LRUs
Michel - Prefer to edit text rather than table
Closed Siobvan's comments, which were actually the result of an email conversation with Larry and making sure we tie 3.5 security measures with objectives and/or activities in chapter 4
Topics that require discussion
When are security measures identified and specified? With respect to airworthiness?
Chuck - What's wrong? What issue am I trying to resolve? Develop requirement to address that. Then look at rigor. Less wiggle room with existing design, but still in product develop process. You don't identify new security measures any time and add them in, you do that when you identify a flaw
Start at top of process, don't want to skip anything
Stefan – in 3.5 we are suggesting you don't have to repeat lifecycle
Michel – we should delete sentences in question (first paragraph)
Martin – you can identify a security measure at any point during process, and if new threat evolves, then we make a design change and start from beginning, don't see reason to define when and where security measures all, two sentences cover possibilities
Stefan - When you identify measures late in the lifecycle, you may need to repeat parts of the lifecycle
Resolution – delete first two sentences of first paragraph, not value added
Other topic of discussion – dependency of security measures
Should there be bidirectional, what assets rely on a security measures for security + what assets security measure relies on for security
No opinions at first
Stefan – useful in safety, but if we don't think it is useful in security, we can delete it
Jean-Paul – need to have bidirectional
Patrick - isn't this good systems engineering? Don't need to be overly specific
Resolution – delete and move onto next topic

Change definition of what dependency is

Summary of Threat Scenarios and Conditions (Cyrille M.)

18 comments, 1 non-concur

Summary of changes – see whitepaper for complete details

- Removed “intermediate asset”
- Removed re-definition of security perimeter
- Reworded subsection on vulnerabilities

Impact is more a security term than a safety term

FHA – if it’s obvious there is no cause for functional loss, it is not listed, no random failures

Leverage off FHA if there is the same effect on aircraft

What can be a threat condition?

Michel – need buy-in from safety people, so need to be careful when rewording these sections

Looking at 3.4 Threat Scenarios section

Michel - Attack not successful, threat scenario still attempted

Philippe - If an attack is not successful, there is no threat scenario

Sentence deleted: A threat condition is the result of a specific threat scenario in a real world aircraft

Clive - Comment on term “vulnerability”, need to be consistent in definition, replace definition in text with glossary definition

Text in Inherent Vulnerabilities section misleading, replaced with new text and better scoped

Threat Scenarios Considerations section completely removed

Clive - Dan took action to update figures 3-10 and 3-11

Break – team picture

Continuation of SAL (Armelle)

Reviewing objectives tables associated with chapter 4

Discussing splits in the table

Dave – inappropriate to have CC listed in the same table, no notion of safety, not done for safety, can’t compare it to DO-178 and such, requires additional work and deserves its own appendix, possibly a table of equivalences

Martin – it’s about assurance that you have the right requirements, and CC is very similar, assuring you have the right requirements and did the design properly. They are not far off. Processes of aviation has end goal of safety, CC has end goal of security, similar

Dave - you made my point, they are different

Stefan – table says this is what we want for security, there are other standards, always will need a separate safety process

Discussing aircraft vs. system vs. item scope

Splitting an objective (Peter Skaves comment)

Might not address all comments on table

Karan – if they are not happy with it, they might bring it up in FRAC/OC

Stefan – we have to live with these objectives, not the regulators

Dave - What matters is if this guidance will be used, if enough companies complain, it won’t see light of day

Companies (people in room) are not complaining about this particular thing

Karan - FAA will reference portions of document in AC

Varun and Jean-Paul currently out of room and can’t comment on behalf of regulators

Michel - Propose we work on comments received, will get back to Peter on comments

Decision – people in room don’t know where proposition to split objective is coming from, move on until Peter is on phone

Making comparison to SOIs (from DO-178) and objectives

Regulators back on room

Stefan - Do we need an objective to show that we mitigated everything that is accepted by authorities?

Already got it with substantiation evidence provided

202A says all risks mitigated
Jean-Paul - Different term, we say “it is treated”, “mitigated” implies a particular solution
Varun – compliance is what you’re really looking at, compliance data is different from sustentation data
Do not necessarily have to submit substantiation data, that means we have to control it, and we can’t
Martin - Identify everything, something might come up later
Stefan - Bad press, can do something not related to safety but still looks bad
Michel – to close out comment, we will add objective in 4.37 Security Certification Liaison Objective that specifies compliance vs. substantiation data, see spreadsheet for wording
Trying to get through SAL non-concur comments before lunch
Comment #868 – propose to call it safety in objective
Comment #870 on O9.11, need to address baseline in configuration management
Martin – baseline is handled by certification, cert data sheet, regardless of objective or activity, we are good either way
Varun - Part numbers tracked after system build, need to redo build to change security requirements, similar to flight control requirements, need a whole new build to change one of those
Adds another layer of complexity and audit and not value added
Stefan - Security measures captured in configuration management system, that way DAL E systems still have configuration management
Stefan - Need pointer to whatever is existing, Phil says he is already doing this even though there is not an objective, would he ever decide to skip it?
Varun – he does it for business reasons, so he will still do this
Martin – still need security and DAL E for certification, if you have an access point, need to prevent unauthorized access
Varun – needs to be a 95% solution
Michel – take a vote on whether to keep original wording or adopt new wording
Stefan – can we please add baseline to address comment
Already meeting it
Varun - What do you mean by “configuration management is robust enough for security?” security should be part of configuration management plan, that’s the key, is security configured? Tracking security versions.
Stefan - If there is no objective, an auditor is not going to look at it
Martin and Varun disagree on taking credit for security at DAL E
Went off topic, then came back to changing objective to "Configuration items are identified, including for security measures, and their consistency managed through a baseline."
Comment #939
Dave – misleading to have traceability without equivalence
Discussing CC vs. DO-178 again
Dave – someone could take what you use to prove failure in CC without going through sys development process, and then you don’t get an equivalence, I don’t want the two compared
Martin – my issue papers reference CC and other non-safety things (FIPS)
Stefan – you will fail cert if you assume you can use this guidance without 254 and such
Dave – representing it in the table is misleading
Edit text in table to clarify?
Michel - Applicant has to do exercise, not the standard
Added “…shall not be taken as an equivalent or substitute…” to address Dave’s comment
Lunch

Discussion of preparation for December meeting and FRAC / OC (Michel)

Looking at comments metrics again
The following categories still have non-concurs:

- Level of threat
- Risk acceptability

- SAL (7!)
- Security assurance

Phil – document has changed significantly, we need to digest it
Michel – will incorporate responses to comments in draft, look for something before December meeting, use FRAC/OC as opportunity to raise any further comments
High priority concerns will be worked out during December meeting
More confidence after this week
Phil - Can next draft come out a week before the December meeting so we have a chance to review and be able to speak to it?
Michel will incorporate comments by priority
Might aim for conditional approval to go to FRAC and worry about editorial comments later
Clive – are there a lot of open comments with Dan's name on them? What is his availability?
Michel – planning to go through them tomorrow morning and reassign as needed
Stefan – make judgment whether comments are straightforward, have merit, etc.
Thanksgiving holiday in between for US folks
Continue with weekly telecons but decide what we want to achieve
Stefan - Talk about security assurance if we don't get through it today
Through in more telecons to make sure we get through it by December?
Responsibility of subgroups to go back to commenter and notify Michel to close comments
Total 10 non-concurs need to be answered and closed
35 high comments
Still a lot of work to do over next couple weeks, need subgroups to help Michel
Philippe – I have a priority that isn't a comment - How are the objectives assigned according to SAL?
Michel – currently proposal? What I put together yesterday?
Stefan – need to know how to restructure chapter 4
Philippe - Objectives split between security and recommended assurance, need to follow safety development process, some objectives covered by safety, how do we trace?
Non-concur, I can't apply these objectives at item level
Dave – if you define something whether item or system as security measure, different process from safety, don't think that's necessary, bigger concern is objectives doesn't have rigor as safety process
Philippe - Not about process, can't apply safety process, point is that rigor of activity, can't apply to software, implementation is security measures
We know what security measures are but what are sub-items?
What are we claiming credit for?
Larry - Is a partition a sub-item?
Stefan - Partition is an item, software item with bounded and well defined interfaces
Larry - Smallest granule where you do the process is a sub-item, I thought that was a partition
Varun - Mechanism between that provides time and space separation
Dave – ARAC directed harmonization on topics
Item definition came from ARP 475A
Assurance item, multi-item, and sub-item definitions came from Dan
Siobvan sent Michel some rewording because multi-item and sub-item definitions contradict
Is a sub-item really an item?
Larry – why are we having this discussion? Going to get pushback from safety people. Requested example from Philippe
Propose to remove "assurance item" completely
Martin - Why did we remove independence?
Larry – safety implication
Martin – didn't we define what independence meant from a security perspective?
Convinced us to put independence back in

Looking at definitions – independence, isolation, and diversity
For those attending tomorrow, meeting will be at EUROCONTROL
Displaying upcoming schedule
Florida is on the books, everything else is TBD
Adjourn

5. Friday, November 17, 2017 Day Five

Discussion of Non concur and high comments (M Kelly)
Section 4-5-3 – Comment 593 – agreement from Mark that it can be closed

Linking security requirements subgroup
Section 3-6-7 – Comment 361 – proposal was to remove the section – agreed – L Hannert remove the section and add new section to 3-4 Threat Scenarios
So a new section 3-4-1-4 is proposed – Need feedback from SC -216
Some minor changes and clarifications were made to the text and agreed that the section can be included in 3-4. Needs to be reviewed by the sub-group and examples need to be reviewed
Comment 809 – section removed vy comment 361

Vulnerabilities
Most is on introduction of vulnerability identification – propose that the subgroup comes up with a resolution

Formatting and language
The talk about no safety effect ios probably more than a language topic

SAL and Security Assurance
First of all the definitions, we now have the four levels – review of Table 4-3
SAL0 Discussion
PW - Request to change systems and items to assets – SAL0
RS why not keep systems and items.
CM – In section 2 – preliminary we have the assets that have the safety impact.
RS – So any system is an asset? CM No.
MM – adds the notes as defined in section 2.
RS – Is there an example of a system that would not be.
RS – when we have special condition – all systems need to comply with the special condition, so if a system is disconnected or not connected, we still need to demonstrate it is okay.
CM - As part of section 2 we identify the assets.
MM – Assets are sources and we also have systems that have no safety effect. So are we missing the completeness for SAL0. Looking at the three objectives
PW has an issue with the authenticity and integrity – Objective could be conducted many ways, so process could do it. Authenticity is probably the issue. Example was given of the dataloader, but is that a special case. So can it be removed? How do you therefore cover dataloader.
PW Could the objective be split into two – authenticity and integrity. Looks like that is not possible so the resolution is we just put the objective as SAL1 and SAL0 has now gone back to systems and items.
PM – Do we remove within the security scope reference.
Objectives for SAL 0 okay

SAL1 – definition discussion – removed the last sentence ‘appropriate’. Back to principals to check consistency. General discussions around asset, measures procedures functions – does the definition appear consistent. Reviewed and amended and now review of the associated objectives. Change robustness to hardening – changed
Objectives for SAL1
Partially applicable objectives - so eight are required, and nine or negotiated, as applicable, replaced with

as negotiated,
Objectives – reviewed – A as defined as gives flexibility that can be negotiated close to SAL2 or nearer SAL0
SS – Do we need a rationale for the As Negotiated – do we need a note for the basis of the negotiation
Are we mixing assignments and definitions?

SAL 2 Objectives review – PM why are SAL 2 and 3 the same for specific assurance aspects – penetration testing – how do we differentiate and can we, not in this document, but do we still need a note about this.
Stefan –has offered to provide a note, need to keep FAA and EASA involved in this - **ACTION**

Activities 6-13 and A6-14 – discussion around whether these are appropriate for aviation, the argument is that yes we are going beyond normal IT systems is that we can't for instance role out patches easily, and it is in line with safety. These are also activities Objective 6-6 tweaked to remove the word structure#
PM what will be the stop point?
Do we need to extend the activities to look at some other aspects – dead code etc. Probably something that the subgroup needs to look at

Do we need independence at risk assessment – at SAL 3 probably required -

Added an additional note that SAL levels are cumulative

Question – are we going to do some mapping beyond assignments and do some algebra relationship that does beyond the assignment principals. It was looked at in DO-356 but was difficulty and robustness difficult to achieve.
At this stage no

General comment for the editorial group – SAL – assigned to measures

CM – Why no appropriate measures for SAL0, there will never be a case as it is an outcome of the risk assessment. - SAL2 – should be SAL3 in the note

MM to send out the assurance draft all final comments on security assurance levels and mapping in next couple of weeks, Final resolution needs to go in the draft at the end of the month.

Principal Two on assignments – when do we need two independent measures – catastrophic only proposed by RS as this is what is done now. Defence in depth argument – maybe you need to go beyond and introduce hazardous for defence in depth.

Two independent isolated security for catastrophic and multiple security measures are likely to be required for hazardous or measures?

SAL 3 - Strongest Security Assurance for security measure. All security objectives
SAL 2 – Advanced/strong level security assurance. Security objectives that allow the use of COTS
SAL 1 - Minimum security assurance for security measures
SAL 0 - No protective effect

Do we have the general convergence on this now, Email to go out to the wider group to review the assurance section as this needs careful consideration by all.
Action Stefan. Appendix H may need to be revisited as a result of this review –

Thanks and closure of the meeting by Stefan
Lunch and close of meeting

6. Main decisions and actions

Decisions		

Actions	Who	When
Resolutions in priority order NC,H,M	All	Before end of November
Testing – Need a explanatory note that there will be a different level of penetration testing between SAL3,SAL2 , SAL1, which we cannot cover in this document. EASA and FAA to be kept in the loop for this	Stefan	
Separate paper to be sent out to the group final comments and changes	All	Telecon 2 weeks final results for draft