EUR 66-18 / WG72-107
RTCA 327-17/SC216-078

St Denis and Washington, 5 March 2018

Summary of the Meeting of RTCA Special Committee 216 (Meeting 37)
EUROCAE Working Group 72 (Meeting 49)
Aeronautical Systems Security

DATE: Dec 11th to 15th, 2017

PLACE: Embraer Engineering and Technology Center
1400 General Aviation Drive
Melbourne, Florida 32935

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

ATTENDEES:

			Dec 2017						
Name	**First Name**	**Company**	**SC-216**	**WG-72**	**11**	**12**	**13**	**14**	**15**
Angermayer	John	Mitre	X					T	T
Call	Martin	Boeing	X		**M**	**M**	**M**	**M**	**M**
Descargues	Gilles	Thales		X	**M**	**M**	**M**	**M**	**M**
Flores	John	FAA	X		**T**	**T**	**T**	**T**	
Freitas	Joacy	ANAC	X			T			
Ganiou	Raoufuo	Transport Canada	X		T	T	T	T	
Gauthé	Armelle	Apsys for Airbus		X	**M**	**M**	**M**	**M**	**M**
Goodchild	Clive	BAE Systems		X	**T**	**T**	**T**	**T**	**T**
Grant	Christopher	UTC	X		**M**	**M**	**M**	**M**	
Hannert	Larry	LCH	X		**M**	**M**	**M**	**M**	
Henrique de Castro	Claudio	Embraer	X		**M**	**M**	**M**	**M**	**M**
Hofmann	Karan	RTCA	X		**M**	**M**	**M**	**M**	**M**
Jing	Owen	Department of National Defence of Canada	X		T	T	T	T	T
Johnson	Dan	Honeywell	X				**T**		
Kelly	Mark	Esterline	X		**M**	**M**	**M**	**M**	
Kerbrat	Anne Cecile	Dassault Aviation		X		T			
Khanna	Varun	FAA	X		**M**	**M**	**M**	**T**	
Kuchera	Robert	BAE Systems	X		T	T		T	

Labay	Marcus	FAA	X		**M**	**M**	**M**	**M**	**M**
Leonardon	Laurent	Rockwell Collins		X	**M**	**M**	**M**	**M**	
Marquis	Philippe	Dassault Aviation		X				T	
Messerschmidt	Michel	Airbus		X	**M**	**M**	**M**	**M**	**M**
Moreaux	Jean-Paul	EASA		X			T		
Morrissey	Patrick	Rockwell Collins	X		**M**	**M**	**M**	**M**	**M**
Newman	Bridger	Airline Pilots Association (ALPA)	X		**M**	**M**	**M**	**M**	**M**
Nguyen	Daniel	Boeing	X		**M**	**M**	**M**	**M**	
Nori	Ravi	Teledyne Controls	X		**M**	**M**	**M**	**M**	
Nyikos	Siobvan Megan	Boeing Commercial Airplanes	X		**M**	**M**	**M**	**M**	**M**
Pierce	Dave	GE	**X**		**M**	**M**	**M**	**M**	**M**
Rosay	Cyrille	EASA		X	**T**	**T**	**T**		
Royalty	Chuck	Aerospace Systems Cyber Security	X		**T**	**T**	**T**	**T**	
Sampigethaya	Krishna	UTC	X		**M**	**M**	**M**	**M**	
Schwindt	Stefan	GE		X	**T**	**T**	**T**	**T**	
Skaves	Peter	FAA	X		T	T	T	T	
Skelton	Brittany	Boeing Commercial Airplanes	**X**		**M**	**M**	**M**	**M**	
Trope	Mitchell	Garmin	X		**M**	**M**	**M**	**M**	**M**
VonGroote	Anna	EUROCAE		X			T		
Waheed	Mohammed	Aviage Systems	X		**M**	**M**	**M**	**M**	**M**
Waller	Adrian	Thales		X	T		T	T	
Watson	Philip	Panasonic Avionics Corporation	X		**M**	**M**	**M**	**M**	

M meeting, T telephone

1. Monday, December 11, 2017 Day One

FAA statement – Varun
RTCA and EUROCAE policy – Karan
Dave - Want to get document in shape for Formal Final Review and Comment (FRAC) / Open Comment (OC), 45 days, this week need to resolve non-concurs and highs
Action items for editor (Michel) at end of week, might need help getting ED-203A into RTCA format for DO-356A
Karan – time it with the TAC, they meet around January 15
45 business days puts it around February 25, in time for a March meeting
Varun leaving early, then Mark will be Designated Federal Officer (DFO)
Dave - Not a lot of work happened between Brussels and now, plow through comment list
Michel – Christmas around corner, need to get document in shape this week, don't expect work done after this week
Karan summarized leadership call last week, concern this document won't go to FRAC, regulatory offices want to go to FRAC and get this in so that it is published by mid-2018
Dave – non-concur should be a company position with good justification, one voice per company
Michel reiterated that the company representative must comment and vote on behalf of the company
Start with overview of status
Michel has two versions of draft document with each position (re: SAL)
Discussed issue of configuration control
Phil - Reverting back to original version will generate same 100 comments
Michel showed comments metrics
Do we want to address new comments? Only if we have time
Dan Johnson submitted a paper, seemed to be meant for main body as opposed to appendix, should we review it during this meeting?
Martin – it seemed to be put together quickly, not ready
Most people haven't read it yet, very late in process
Michel – we should at least review it
BASOO should be on phone tomorrow
Need to find out when Dan will be on phone to present his paper
Larry – do we want to package what we have or add content to it? What is the objective?
Varun – it's your doc, you decide

Appendices
Discussed multiple methods in appendices
Dave said there shouldn't be more than 2
Siobvan pushed back, can't force Boeing to do Airbus method or Honeywell method
Clarification that this is a guidance doc
Martin – people should be able to use this and come to same answer, not reality
Dave - 326A should be standalone, but it is hard to use without additional guidance
Michel – don't know how to deal with all these last minute inputs
Patrick – we should revisit removing all the company methods from the appendices, will shorten document, resolve inconsistencies
Martin – let's take a vote before we get too far
Make sure we are clear about what appendices we are talking about
Appendices D (part of it at least), E, F, G, and H are contentious
Michel – on other hand, appendices provide additional detail
Varun – shouldn't that be negotiated with regulatory authority, everyone's processes are slightly different
Martin – will be more acceptance from companies if we remove appendices
Stefan – I see Varun's point, however, what if someone needs to see how to use activities and objectives or

what a threat tree looks like
Martin – everyone understands safety, don't want safety people using this to do security and following cookie cutter approach
Audience has to be knowledgeable, not lay people
Chuck - When Cyrille or Varun work with companies, they work with experts, safety assessment process starts with safety people being skilled
Should approach security the same way
Cyrille – formalizing part 21 document…
Clive – What does this mean for avionics suppliers? Don't want to learn 4 different methods!
Patrick – up to supplier to decide if they should have a companywide method based on OEMs they work with, we are still arguing this because this is an evolving field
Stefan - Products that bolt onto more than one aircraft, don't want to do something different for each OEM, point of this document is to have something that resembles same language
Varun – key is to meet security objectives and negotiate details / process with regulator, each applicant has their own take on DO-178 and that's a good thing
Dave – if you have prescribed methods, pressure to use them, more appropriate to take out company specific
Varun – this is not a catalogue
Michel – why remove them? Referred to ARAC
Dave – remove because they are causing non-concurs
Michel – not enough disclaimers on them?
Siobvan – I don't see a newcomer with no knowledge of security using this document to do a certification, should already have security expertise and be knowledgeable of security methods and processes
Varun and Martin discussed companies being big enough to do security or at least contract someone to do security, should have security built in product to be certifiable
Discussed supplier perspective
Patrick – I know how to work with Boeing, I know how to work with Airbus, don't need prescription, or should we throw in a Rockwell method?
Ravi – the methods in the appendix are supposed to be for references, aren't required to use them…
Patrick - Until ACO says you do

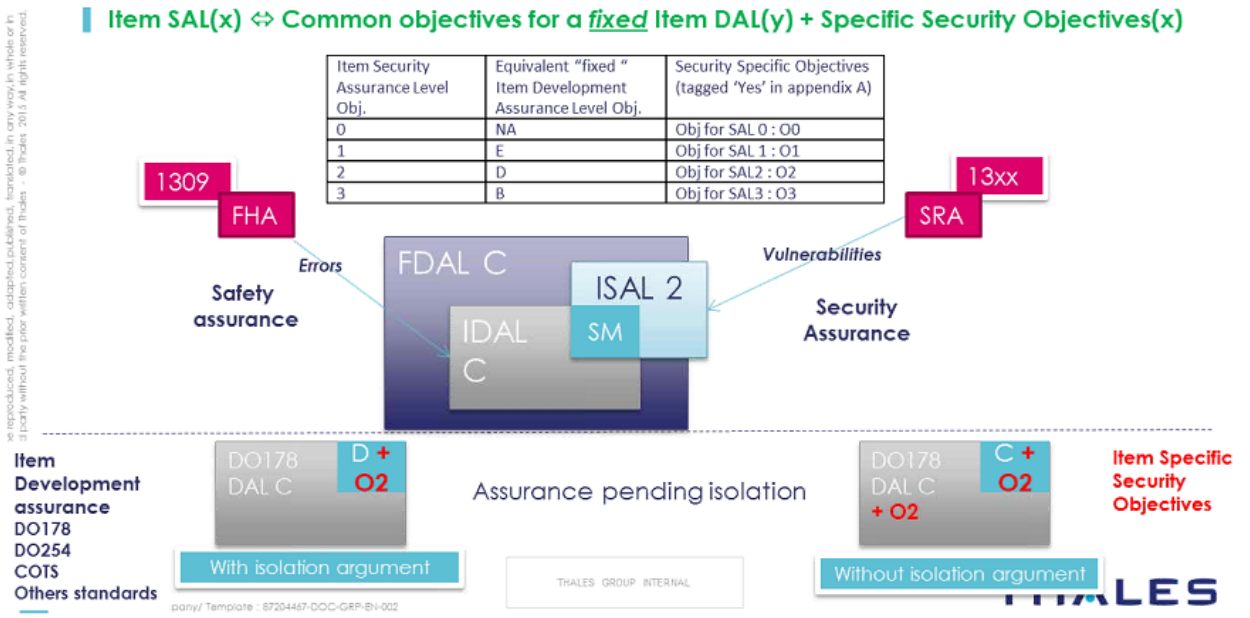
Vote on whether or not we delete the four appendices will be tomorrow

SAL Topics
Dave - SAL is a topic we have a lot of issues with, avoid long examples unless necessary, come up with agreement on principles of what SAL should do for us
Michel – want to formally close non-concurs
Phil – yes, can close non-concur against appendix H based on current draft
Looking at current SAL table
Phil – still need edits re: partitioning, sub-items, etc.
Gilles - Is it a problem to say a security measure is an additional component of an item?
Martin - Up to assessor to define, if security measures has dependencies, apply SAL to those
Clarification – is only catastrophic in need of two security measures?
Martin has non-concur, major or higher need defense in depth, see ARAC report
Stefan – no single point of failure for catastrophic only, lower than catastrophic should have more than one measure, need to think about what we write here
Martin - Not more than one measure, more like more than one layer, a measure can be part of a layer
Layered defense does not have to be on same system, just needs to be on the threat path
Martin - Need to include operational considerations
Michel – we say security measures don't need to be technical here, they can be operational
Stefan – comment from Dave earlier that we shouldn't be taking credit for operational, need clear rules in

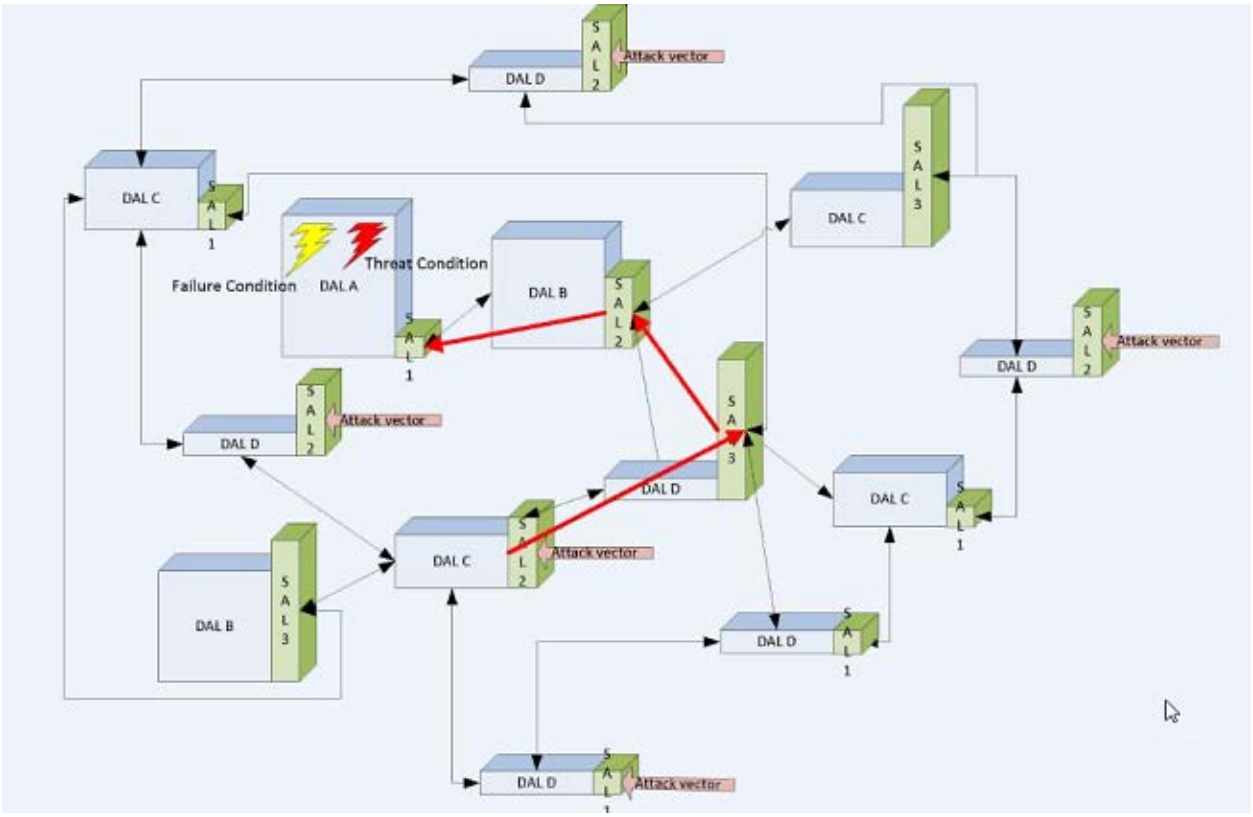
main document
Martin – need both technical and operational, otherwise someone with admin access can override technical controls
Chuck – who do you decide to be an insider? Used to be part of likelihood approach. Need to have insiders and specify access. Can't control at sys level, control via background check. How do you decide credit on controls outside airplane?
Principle #2 on two security controls – catastrophic only or hazardous and above?
Martin – ARAC drew line at major, need to enforce layered defense or major and above threat conditions
Discussing Michel's example to sort out principle #2
Phil - Independence clause might cause a change in architecture
Patrick - Input validation on data twice? Is this useful for system? Seems excessive
Don't want to get into a situation where you do everything twice
Martin - Concerned with major or higher threats unless you consider propagation, need layered defense
Minor threat level – don't need more than one layer of defense
Major and above – need more than one layer
Two layers a major needs is different from two layers a catastrophic needs, that's the difference, that's how we can use SAL
Validating twice discussion
Laurent – validate input, then validate again after?
Martin - Two systems, each provides a layer, then do input validation on each system because they were created by different people
Major is significant increase in crew workload, two majors can be catastrophic
Phil - Authentication in combination of data validation, count as two?
Chuck - Problem is you're treating dataload as a sub-optimal point, lots of options for ensuring airplane is in correct configuration beyond software load
Patrick – trying to find common examples to test against this
Michel – come back to point, how many layers required for what
Martin - Currently regulations say multiple layers (special conditions call out multi-layer defense), are we going to change that?
Varun - One approach is take conservative position, see how it goes, then revise document later if needed
Another approach is take liberal position
Make reasonable assumptions
Dave – could say it depends on vulnerability, but that's a much larger discussion, care about everything but DAL D and E
Varun – architectural considerations taken in defense in depth
Catastrophic and hazardous - yes, need defense in depth
Major still under discussion
Cyrille's opinion?
Martin – if it is not required for certification of a major system, he loses leverage, security will lose out to cost and schedule
Brittany – if cost to implement security is less than cost if you lose system, leadership will decide against security
Easier to make justification if it's a security certification requirement
Mitch - This document is not the place to impose business requirements
Varun – down to architecture and what applicant negotiates with regulator
Michel – one layer can be enough depending on security measure
Lunch
Continuing SAL discussion and resolving non-concurs relating to SAL
Decision regarding principles – need two security measures for catastrophic and hazardous, principles #2 and 3
Martin is OK with all principles now except #8 re: SAL 0

Clarification – if threat condition is “I don’t care” or DAL E, then you’re done
Now they are OK / accepted
Dave had a comment against the note before the tables and what it implies, should be reworded
Leveraging DAL assurance for SAL compliance?
Development assurance supplement considerations: In an existing safety development process at the highest design assurance… - disputed, discussing if this is too generic or too details, what exactly does it mean
Phil - DAL C requires source code and SAL 2 doesn’t, are they the same?
Dave - This is where the problem is, how many people in the room agree?
Equivalent if they have the same hazard or impact level
Varun and Brittany - Have to assure yourself that controls in place are effective against threat
Martin - Having the right requirement, verifying that if functions properly
Earlier, wanted security to be separate
Assurance that security measure is effective
Dave agrees, however, high SAL vs. low SAL doesn’t mitigate attack (either effective or it isn’t)
Patrick - Higher level, checking requirements for correctness, at lower level, you aren’t
Dave – can have this in here, but don’t need it, first 4 objectives pointless (O3.1 through O3.6)
Reviewing Thales proposal for harmonization

ED203A/DO356A: Proposal for harmonization



Peter – sometimes a safety measure will cover security
Michel - Security measures propagated along network and threat paths, not highly critical systems
Martin brought up example where someone loaded an updated part (as opposed to malware), and it caused an airplane crash. System didn’t detect it
Having said that, some people said they hadn’t heard of it, part 25?
Chuck has issues with one of the slides in Thales pitch



Larry - Even without security, DAL D allowed to be DAL D because its effect is mitigated by B and A boxes
High DAL boxes can use inputs from low DAL boxes, that doesn't mean we need to bring up the DAL of those lower DAL boxes
Michel to Chuck – does this mean every system in the aircraft should be DAL A?
Martin – every input is supposed to be validated for effect on system, however, when you add intelligence and reality, not every single input is tested
Varun – classes of test that cover range, don't have time otherwise
Martin - Difference between intelligent threat and software error
Peter – wondering how this will actually work when docs published, pictures are different regarding functions and DAL, right now policy statement about external connectivity
Plan for scoping of this?
Varun – figure mean to show varying SAL and DAL as part of the same box, distributed controls, controls not necessarily on perimeter, rather spread throughout
However, have seen mostly controls on perimeter in real life
Michel – in practice, gateway security measures
Look at policy statement, what happens when you add another box to architecture, how does it affect the rest?
SAL not a process, rather it is a set of objectives to put in existing process
Michel – Airbus defined in 2008 for A350 development, in supply chain as well, experience that this is a useable approach
Not best answer for everything, but it is possible
Ravi – when this is published, do we need to show for regulators what is the SAL and how we came to that? Yes
Larry - Safety mitigates you want to take credit for security don't have a SAL
Closed Dave's comment re: note
Continue to go through SAL comments
Martin – objectives O7.1 through O7.5 should be required, not as negotiated
Varun – as negotiated may give you leeway

Stefan – this way, it's not all or nothing, it's what is appropriate
Martin – if you're taking security credit, need to do these
Phil – recommended, not required, for secondary measures
Martin – no problem with refutation objectives
Ravi - Is there a case where preliminary risk assessment not required
Martin – yes if not taking credit
Dave – 326 says you should always do guidance. What does this table mean?
Michel - If objective doesn't apply, you don't have to show correctness / completeness
Dave – if you follow all objective, no 326? Objective to do the guidance?
326 has objectives with inputs, outputs, and actions, but they are not in tabular form, will this be confusing?
Looking at 326 security assurance and security aspects of certification (appendix A)
Michel – these 326 tables are for information, not mandatory part of document
Dave – 326 tells you more of what to do than tables in 356
Michel – these are activities, might be missing some here
Patrick asked about operator guidance in 356
Michel - We have an objective to provide guidance
Martin - Keep access open to monitor new threats
Patrick - Not opposed to that, but it's not there today
How is this different from 21 part 3? It's not
FAA Mark - 21 3 can handle confidential, be careful how it's transmitted
Martin – redundant objectives re: security guidance to operators
Patrick – does Boeing, Airbus, etc. have secure communication and distribution system?
Brittany – company should already have that in place
Stefan brought up part 21 and EASA horizontal rule, this will come up again
Decision to remove this objective, not going to tell a company how to securely manage its proprietary information
Dan Nguyen – Can't have good vulnerability process without detecting vulnerabilities, contradiction in objectives
Mitch - Nothing bad, just how much do we want to impose on ourselves for relatively low assurance systems
Dan N. - Low SAL on high DAL?
Mitch - That's what "as negotiated" is for
Brittany – how are you capturing this? Cert plans? Yes
Granularity is not there
Martin – meeting minutes
Brittany – negotiation adds weeks of work
Martin – just add it as requirements within company
If you leave this one as an "A" for "As negotiated", need to do that to other corresponding objectives
Phil – more appropriate to have A
Stefan – applicant must justify how much they are doing so that we know A doesn't mean nothing
Patrick concerned about "capability to monitor security measure effectiveness is established" and what it implies
Martin interprets it as time goes on and you have more insight and tools, you re-evaluate to see if security measures are still effective
Do you do that now? yes
Not test, but assess
Example – WPA2
Patrick – if there is already a process for this…why are we calling it out in the objectives
Don't want anyone to think they need a new separate process
Varun – monitor what supplier has changed, plan in place, all the major companies have a plan in place

Dave – have ways to handle field conditions as well
More discussion on capability to monitor
Adjourn

2. Tuesday, December 12, 2017 Day Two

Informative Appendices
Took a quick vote of who is for removing appendices with methods and who is for keeping them
3rd possibility offered by Phil is to put appendices into a whitepaper, that way they are not in the document but they are not completely deleted
Mitch supports this too, that way they are available for reference
Doesn't need to go to FRAC
Patrick supports it – FAA?
Varun & Dave – yes, then there would be AC for three published DO documents, FAA will be aware of whitepaper and its contents
Michel – don't have that many non-concurs against appendices, difficult to follow with example methods in appendices, concerned with needing to find other document somewhere else
Cyrille – can deal with via AC, Varun agrees
Michel – as editor, don't want to address this week, handle whether or not we remove appendices
Siobvan – if we are leaning toward removal, do it now before FRAC, otherwise you are giving the public a 300+ page document with appendices that could cause confusion
Also, is there a tool on the RTCA or EUROCAE websites where each company can submit an official vote on whether or not to remove the appendices
Ravi – shouldn't remove for reason of lack of understanding, otherwise you can eliminate SAL discussion
Mitch – not just lack of understanding, don't want someone to think they are constrained to those four methods
Varun - Jean-Paul would like appendices in document, EASA position
Larry – not unique to this group where people are concerned examples are the only way, have been able to resolve in the past
Varun – fundamentally a training issue
Mitch - Can AC allow us to tweak methods?
Varun - Yes, you always have that ability
Security is new and relatively unknown
Mitch – OK as long as AC or something official gives us permission to do this
Martin – what about all the methods in one big appendix?
Discussion, comparing to DO-178
178 still has appendices
Martin – ask two experts, not necessarily security people
Dave – we are only there for safety, a ton of safety in process already, not a whole new thing, needs to relate to what we already have
Martin – how to do security assessment is brand new to industry
Krishna – In light of recent hacker community interest in aircraft vulnerabilities, what if appendices are used as potential misuse cases?
20 objectives
Now, group is leaning toward adjusting disclaimer wording at the beginning of appendices to address concerns from suppliers

Non Concurs
Martin OK with closing his non-concur against SAL
Continuation of resolving / closing non-concurs
Bridger (explaining non-concur) - When pilots go through training, learn everything system on aircraft. Seeing special condition re: wireless access points and connectivity to these systems. Pilot will need training, knowledge, and cert to understand interactions with airplane and flight operation, nominal and non-nominal. Pilot may not need to do anything but will need to be aware
Varun – new connectivity, but not new systems. Don't want to interfere with pilot workload. If there is a cybersecurity event on an IFE system that takes out IFE or something else, there is nothing the pilot can or will do onboard flight to solve that
Bridger – can turn it off. If pilot needs to act different, need to know how
Varun – truly believed that pilot can't trouble shoot in flight or on ground. Maintenance can't troubleshoot, rather they replace parts
Michel - Responsibility on end user (don't open attachments), experience is user can't make decisions because he is not the expert, burden should not be placed on pilot, he has higher responsibility, should not come into position where he needs security expertise, aircraft systems should be able to protect themselves
Chuck – when you look at effect or lost system, you don't know why it occurred. If you do, then you already know the attack vector in sys design. You either have all the info or you don't and should not bother the pilot and play detective
Martin – if messages are spoofed, could you tell off the bat that the messages are bad?
Bridger - With ACARS, there have been messages from a bad source, and the pilot reaches back to company to confirm
Peter – flight crew needs to know what failed and any action they must take. They don't need to know why it failed
Martin - What if your comms where denied? You can still fly airplane no problem
What about software defined radios? What could they do and is it a big deal?
Looking for confirmation from a pilot that you can still fly the plane
Mitch - Always have loss of comm procedures
Bridger and Varun in agreement now, just want situational awareness
Closed non-concur comment

Viewing Mitch's proposal for disclaimer note at beginning of appendices in an attempt to keep them and address concerns from the group
Changed "means" to "possibility" to address Stefan's concern that "means" will imply means of compliance
Michel copying wording to other three appendices
Martin non-concur on SAL – proposal to change the table

Risk Acceptability Matrix
Martin – I know what is red / high in my company, but not comfortable with interpretation in table on risk acceptability matrix
Minor shouldn't always be acceptable risk, need a separate chart for when a minor system is used to propagate a threat
If threat scenario is minor, don't need to do anything
If you evaluate systems independently, are security measures sufficient, looking at minor system in threat path
Patrick – implementation choice
Martin – need asterisk, when used in conjunction with higher level threat scenario
System vs. airplane level
Phil - If you have a measure that is minor that is in the path of something major, then the threat condition

is actually major
Chuck – issue is that anything below major doesn't matter
Martin – look at 1309 for safety and table is different, not always acceptable for a minor system
Most people in room are OK with risk acceptability table
Chuck – kind of with Martin on this one, trying to write exclusion that is not consistent with rest of industry
Martin – will try to compromise and consider minor in threat path to major or higher system
Phil reiterated position
Martin – what about system only assessment? Layered protection in system?
Patrick – depends on end state, what is max possible effect? Per table, if max possible effect is minor, don't need to do anything
Bridger – we may need another table
Martin – go back to 202 and 326 and say you need to work system assessment first
Siobvan – someone mentioned using two table before, this would be in line with DO-326A / ED-203A as that document differentiates between system and airplane level assessment
Or…just add Martin's asterisk to clarify
Michel made a first pass at clarifying the minor & very high box
Mitch – not necessarily a system vs. airplane issue, focus on propagation
Phil – asterisk words more confusing
Siobvan sent alternative wording: If a minor or lower system is in the threat path to a system that is major or higher, then the risk is not necessarily acceptable and there are further considerations as the true threat condition is actually major or higher.
Mitch – are we trying to include words that are already in the policy statement?
Phil – take out middle part of new wording
Now: If a minor or lower system is in the threat path to a system that is major or higher, then the true threat condition is actually major or higher.
Peter – copy and paste policy statement instead, don't reinvent the wheel
Martin – interpretation inconsistent with policy statement, not clear here, people will make the mistake
Rulemaking will supersede all this
Martin – shouldn't have to worry as long as you flow the correct security requirements to your supplier
Table discussion for now, won't change document unless we get general consensus, can handle via comments during FRAC period
Daniel Nguyen working on wording to provide later, good to get fresh perspective of someone who hasn't been in previous committee meetings

Dassault Non-Concur Comments
Moving to Dassault comments against document while Anne-Cecile Kerbrat is on the phone
Looking at comment on security verification objectives
Also, security refutation activities (see comments spreadsheet for complete details on status and resolution)
Michel - Not sure making activities mandatory is a good solution
Stefan - No, will get more comments if you do, that takes flexibility away
Martin – is definition of refutation being provided by activities? Is the problem the definition?
Michel – propose we improve objectives, as much as we can this week, then will be continued in open consultation (OC)
Lunch
Continuing comment sheet
Another Boeing non-concur, this time against 3.1.2, OK to close per resolution
Next non-concur is from Peter Skaves regarding COTS, OK to close per resolution
Next one also from Peter regarding assurance, OK to close per resolution
Next one from Chuck

Objective linked to security, difficulty in harmonizing SAL
Dave - Additional people have comment, difficult to fix ahead of FRAC, might need different set of tables
Document cannot be easily fixed, no resolution to the non-concur at this time
Michel – can we still move ahead and go to FRAC? Yes
See what rest of aviation industry thinks during FRAC
NC against table 6-45, does table still exist? No
Dave – we resolve this by adding this sentence to the tables: If you do a safety process, you cover objectives in this table
Additional security process…or skip some of it if you already have safety process
Dave doesn't think Common Criteria (CC) applies, but that is up for discussion
Don't have to use CC for justification, CC not at same level as other documents listed
Do we want all this complexity?
4 NC comments on appendix
Got through NC comments
Michel - Many high comments – should we start them or discuss any barriers to going to FRAC?
Mitch – we should discuss meeting and milestone dates for 2018

FRAC process and meeting dates
April 9-13, 2018 in Paris for FRAC / OC disposition meeting
May 14-18 in DC for second / final FRAC / OC disposition meeting, committees approve document
If we want to make June PMC, need to hand over document by May 24, RTCA editor needs it earlier to put it in RTCA format and put on finishing touches
Next PMC is in September
Next milestones and possible dates…

18. Dec 2017	DO-356A/ED203A FRAC/OC Ready version to RTCA/EUROCAE PM
08. / 22. Jan 2018	DO-356A/ED203A Begins FRAC/OC
23. Feb / 09. Mar 2018	DO-356A/ED203A FRAC/OC Review Period complete
05. Mar / 29. Mar 2018	FRAC/OC Initial disposition by Authors distributed to SC-216 / WG72
12. – 16. Mar / 09. - 13. Apr 2018	DO-356A/ED203A FRAC / OC Disposition Meeting (Paris, EUROCAE)
29. Mar / 30. Apr 2018	DO-356A/ED203A FRAC Comment resolution proposals completed
09. - 13. Apr / 14. – 18. May 2018	Final DO-356A/ED203A FRAC / OC Disposition Meeting (DC, RTCA)
*07. May / 25. May 2018	DO-356A/ED203A final version to RTCA/EUROCAE PM

Week of the 19-23 March also raised as possibility for next meeting

Stefan raised the point that the comments that we still have questions on, such as DAL, SAL need to be worked on whilst FRAC starts and should be resolved before we have to resolve the FRAC comments so they can be incorporated, this will require commitment from the group.

Any blockers to voting yes for FRAC / OC – none raised at meeting

Bridger – I have one non-concur against chapter 6

Risk acceptability Matrix
Martin – we have the new sentence to put before risk acceptability matrix:
The risk acceptability is determined based on Threat Condition severity and Level of Threat of a complete end to end threat scenario.
Michel is good with this statement
Can now remove the asterisk statement, changed sentence before table addresses comment
Close Martin's non-concur

Plan for tomorrow – look at level of threat, risk acceptability, and SAL again when Dan is on the phone
Peter – some of these discussions are in other documents, agree with Chuck
Alpa paper
Team dinner

3. Wednesday, December 13, 2017 Day Three

Dan Johnson will join meeting 10am-noon
Jean-Paul Moreaux (EASA) and Anna VonGroote (EUROCAE) will join meeting at 1pm
While we are waiting for Dan to join, going through high comments in spreadsheet

High Comments
All terms used in document have been added to glossary
Discussing definition of security
Michel - Its own concept, we look at security for safety purposes in this document, but it's more than that, defining security to mean only airworthiness and safety of aircraft might be too restrictive
Security measure shouldn't only exist for safety purposes
Security assessment methods can be used for safety as well as other security purposes
Patrick - Refer to ARAC report, unauthorized electronic access
Martin read excerpt from FAA Network Security issue paper to help with definition
What about EASA CRI definition?
Michel – EASA refers to definitions in document
IUEI excludes physical security
Martin – I know domain model isn't accepted by everyone, but ACD and AISD are of concern, from ARINC 664 part 5
Dave - Don't need to do anything beyond IUEI, but you can…and you can take credit for it in your assessment
Not necessarily clear in document
Martin – we should change security to cybersecurity
Dave explaining Chuck's comment - In document, it might mean wider scope in some places and tighter scope in others, and use of term security is not consistent
Varun – if someone gets this document and doesn't understand security, we have bigger problems
Martin – if someone gets an issue paper and have never seen this stuff before, they need to hire or contract expertise
If it's a small company, not as feasible
Chuck on phone, definition edited, comment closed
Dan on phone

FRAC
Michel – strong desire from several organizations to go to FRAC / OC, objective is to get rid of all disagreements that would prevent us from going to FRAC, if Dan has any, we should prioritize those
6 non-concur comments, go through from top to bottom?
Dan – would like material that he just submitted to replace existing appendix
Varun – is it important for going to FRAC?
Dan – yes
Informative appendix F
Reviewing Dan's rewrite of appendix F, very different, assigning numerical score

Appendix F
Dan – most of page count is a fully worked risk assessment, can remove some of that detailed info if needed
Michel – my main concern is that there is a lot of new material, don't see direct link to likelihood method in existing appendix F
Dan – using 10 point scale to express level of protection / threat and severity that come out of likelihood method to determine final risk acceptability
Martin – removing probability so that it is not mistaken with safety
Michel – we had proposals to remove appendices, but then we decided to add better wording to disclaimer, some members are not comfortable with so much detail even in informative appendices
Dan – one request was to have a complete example
Michel – good to have material, other point is that Monday group wanted to discard version from Friday, go back to version from Monday because there was not enough time to review new stuff, safer approach is limit how much new material we have
If we replace a whole appendix with new material that no one has time to review…
Varun – this new appendix is what people will see in FRAC / OC, can comment then
Those who have seen it think it is an improvement
Martin – some stuff to work out, but nothing that can't be accomplished during FRAC
Dan - More potential to pass under revised version, clears up inconsistencies
Michel will make this change to the appendix and we can review later
Larry – do we need to review this before the FRAC / OC vote tomorrow? Yes
When to vote on FRAC / OC?
Thursday morning 11am, better for Europe, also a few people are leaving early
Martin – after vote, is document locked in?
Karan – OK to still work editorial comments, otherwise Martin is correct
Dave – whatever the document looks like end of week is what it is, Michel is not working it further
Michel - Group decisions, 1) do we want to go to FRAC / OC and 2) is the meeting done or do we want to work minor issues that don't affect FRAC decision
Martin wants to make sure that people who vote and leave are covered
Appendix good, switch to comments

Non-Concur
NC against 2.5.1
DAH responsibility to set up continued airworthiness guidance
Dan – look at activities that expand on these
Purpose of original was to ensure we have a complete and correct list
Varun – once plane delivered, airworthiness is responsibility of operator, not DAH
Needed to change wording as a result, DAH can provide guidance, but it is the responsibility of the operator
Do we need to repeat it here?
Stefan made it a non-concur to ensure the two sets of responsibilities (DAH and operator) are completely separated
This is a competing non-concur
Dan – they aren't completely separated
Dave – Dan, can you review the new wording?
Varun - Nothing precludes DAH from their responsibilities, they have to do it
Dan - Issue is about what kind of info needs to be documented by DAH
204 is not an ICA doc, it says what operator needs to do
Varun - Limitations to security controls -> limitations section of ICA
Martin - Is the problem that some objectives not seen as responsibility of the DAH?
Dan – why did you delete the 2.5.3.1 material on that?
Looking at deleted text

Deleted because Stefan thought it overlapped with ED-204/DO-355
Martin – isn't 355 for operator?
Mark – there is some interface with DAH
Varun – there's a part that goes here and there's a part that goes into 355
Dave – needs to determine that
Already determined
Dave – if we added 2.5.3.1 back in, does that address comment?
Dan – no, there's more needed
Stefan is sticking to his comment, that they need to be separate
Not going to block FRAC, but going to make comment again in the FRAC, have already had these conversations
Dan and Stefan disagree regarding whether this text makes the document consistent
Michel - Should prepare to work out better proposals for this topic during FRAC period and engage subgroup for this, subgroup alone won't be able to resolve, look to operational side
Varun – I thought we were going to leave this in and wait until 355 committee reconvenes
Dave – someone can write a dissenting opinion if one is necessary
Finished going through Dan comments, anything else that we need to discuss?
Dan – Still need to discuss SAL and DAL
Michel – supplement approach is included in SAL assignment
Can assign SAL equal to DAL, looking at objectives
Or you can go other way and assign SAL independent of DAL -> independent approach
Both concepts should be presented in doc
Martin suggested writing a supplement to what is already in DO-178, ARP, etc.
Michel – proposed before, but we can't do it alone, would need to engage all those other groups
Won't be able to do that
Dave – don't need to repeat material, just add touch points of where security interacts
Patrick - Minor rewording can advise reader that this is a method to augment existing process, don't need to do this before FRAC, can do this as part of FRAC
Reasonable path forward?
Dan – point is how do people feel about this document?
Dan - Can we submit multipage solutions?
Michel – you need to convince group you need such changes
Dave – Fair to submit whatever you need to
Michel – need proposals that move us forward and not repeat previous discussions
Dave – not going to get your resolution unless you put your material up
Lunch

FRAC and Schedule
Anna – original idea is that we wanted to report back to PMC and TAC
PMC before Christmas, TAC in January
We deviated a little from process if there are dissenting views in working groups
RTCA and EUROCAE management feel we need to move to consultation and a more formalized procedure, recognize there is still a lot to be done, get comments into the open
This approach was discussed with chairs of PMC and TAC
Long story short – they want us to go to FRAC / OC
Karan – we made a lot of good progress this week, consensus building wording in doc, going to decide tomorrow / Thursday at 11am whether to go to FRAC / OC
Might be one or two who do not think we are ready to go forward
Michel – missing feedback from Dassault
Anna – Dassault is OK with moving forward with FRAC / OC
Also, chairman of TAC is from Dassault, so this aligns

Discussion of schedule, timeline, and process
There were two schedule options
Varun – FAA preference is the earlier of the two to get the document out mid-June 2018, it's not a show stopper if it slides, but he needs to give his organization a heads up
If doc changes significantly as a result of FRAC, it will be more complicated
Michel – if we get consensus now, we can open for FRAC / OC in January?
Anna – yes
Michel – in that case we will go with the earlier schedule
However, if there isn't consensus and need to work out issues, will need to wait until TAC and possibly go with later schedule
Next meeting dates will either be March & April or April & May
Martin – schedule is tight with existing comments, how are we going to address additional comments in FRAC / OC?
Karan – that is our fear too, sometimes there are few comments and sometimes there are many
Open to public, but are there comments we can ignore?
Notice not published in federal registry
Martin – a few airlines want to know when it's open for comment
Karan – that is fine, many airlines are RTCA members, Karan will send to points of contact for those airlines, they can't download, but they can look online
Late comments not accepted
Michel will post schedule after vote
Moving back to comments

Comments Review
Filtering by name, starting with people who are leaving tomorrow, whether they are the commenter or part of the editorial group
Siobvan had comment against likelihood appendix, Ravi and Dan in that editorial group
It can be closed as OBE because Dan has replaced that appendix with something completely different
Michel – if there are comments that are still open, up to comments whether or not they carry over to FRAC / OC, the committee isn't going to carry them over for you
Dave – that means everyone needs to read the document as it is at FRAC and decide if the comment is still valid
Continue to go through resolution of comments with people who are present (see comments spreadsheet for status and details)
Discussion of whether or not is appropriate to refer to classification of data, this document is used mostly by commercial, however many participants work on both military and commercial side, and those sides have different data markings and treat data differently
Discussed protecting data and systems from insider threat
Discussed Siobvan's comment against B.1.5 and tables 6-10 and 6-11
Was a language issue, not a math issue
Second column in table 6-10 says "Maximum Combined Effect", but really it has to do with how much credit you get, not means to be cp/cw/ce
OK to close comment
Patrick brought up concern with A12.1

A12.1 Vulnerability identification and evaluation activities have been put into operation, to be performed continuously during production and operation lifecycle phases for products that could lead to an airworthiness security impact
We agreed that the word "continuously" could be troublesome. This is a good practice, but what is meant by continuously? It can be anything from reviewing your architecture when a new vulnerability comes up to having a whole team of people dedicated to continuously evaluating architecture and software for

vulnerabilities and rolling out patches
Replace word continuously with throughout?
Is it in anyone's issue papers?
OK to change word if it still aligns with objectives
Going through Chuck's remaining high comments
Closed Bridger's (ALPA) non-concur against chapter 6
Group comment on security assurance OBE, can close now
Going through more comments on security assurance
Dan still has 30 more high comments!
Do we need him for the discussion?
Martin – Dan didn't indicate that was going to vote against FRAC, any benefit to going through these without him?
Michel – high comments raise concerns, also some comments left from Dassault
If agreement within group on how to resolve, can make the changes
Continued going through comments with remaining time (again, see comments spreadsheet)
Martin - someone at FAA once said you can't have independence in same company, however, we think that you can within the same company if you have a different team designing and a different team testing
Marcus (FAA) – Agree
Patrick – different levels of independence
Michel – business models change, smaller companies get bought
Marcus – also consider what you're testing
Adjourn

4. Thursday, December 14, 2017 Day Four

4.1 Notes from Meeting

Varun went back to Seattle, Marcus is now the DFO for the rest of the plenary
Planning to vote today at 11am but Dassault is not on
If we postpone to Friday, we will lose more participants
Martin – does it have to be a unanimous vote to enter FRAC?
Karan – no, not necessarily
Michel – don't need to vote at the same minute, OK to have most voting today and Dassault's tomorrow
Dave - Should we still have telecons? For info purposes. Might be good to have telecons for subgroups to resolve remaining disagreements
Probably won't have another one until end of January
Dassault was contacted, they have no opposition to going to FRAC / OC
Received follow up email from Philippe Marquis later: "I confirm that Dassault Aviation accepts to enter into FRAC/OC at the condition that our NC and High comments will be addressed during the FRAC/OC period."
Michel went through changes he made to document last night as a results of this week's comment resolutions and discussions
If anyone has any issues with document they want to discuss before FRAC vote, bring them up now
Martin – SAL DAL is not going way. Seems like we are talking past each other. Can work it out later
Dave – I can set up a subgroup telecon on this topic
Martin – some say DAL+, some say SAL, we mean the same thing, safety is going to perform safety processes regardless
Dave – if you have a DAL D system that you want SAL 2 or 3, then you may have disagreement
Looking at Dan's new appendix write-up
Martin – still pretty rough, but we can make comments on it as part of FRAC

Discussed FRAC process
Shouldn't have competing comments from same company, they expect us to work out internally what our company position is and submit our comments
Dave – need to have proposed resolution, don't leave it blank
Karan – if you don't fill in the form completely, you can't upload to RTCA
Impact on airworthiness vs. safety of flight or impact on safety (new wording)
Martin – if we change it, do we lose meaning?
Michel – when we evaluate vulnerabilities, we look at risk assessments and impact on safety
Continuing to go through remaining comments in case we can make progress while we are waiting for voting time

Discussing testing of COTS
Michel – there would be different testing on COTS, but not necessarily more testing, testing is tailored to the COTS, open debate over whether it can be more or less
Martin - Refer to WPA2 KRACK, algorithm used on high and low assurance sys, assumed to be secure
Patrick - Testing might not have found it, spec was wrong
Stefan - Higher assurance, more rigor, more testing, expect to do more testing at SAL 3
Dave – change objective tables, level of effort of SAL is different
Needs to be reworded to be sufficient
Stefan - Otherwise, you would have to take 178 approach
Martin - At security conferences, more interest in hacking hardware and how you do that

Michel – currently no guidance on this
Martin – then does the note even help?
Patrick – many raised point if companies are mature enough to get anything out of this document, education vs. guidance
Martin – since aviation security is new and evolving, that means education is acceptable in this document? Note is neutral, OK to remove

Discussion on going to FRAC
Dave – technically not a "vote" more like a consensus, more than people in room and on phone reviewing this
Will take show of hands around room
If we decide to go to FRAC

- 45 day review period
- Comment sheet, need justifications and resolutions
- All comments will be considered, everyone gets a say

Clarification for John Angermayer – we do not expect someone who is not knowledgeable of security to use this document, some knowledge is expected
Michel – most people in room recognize this is a standard that will develop over time
Unanimous yes to go to FRAC / OC within the room
Unanimous yes around the phone to go to FRAC / OC
We're going to FRAC / OC!!!
Technically, RTCA, EUROCAE, FAA, and EASA do not get a vote in FRAC / OC
Varun – push to publish document by mid-2018, appreciates everyone's hard work
Schedule to meet this deadline:

SC-216/WG72 Proposed Schedule

May 15-19, 2017	Joint WG72 / SC-216 Plenary (DC, RTCA)
May 29, 2017	Provide comments on security assurance (chapter 4) paper
June 26, 2017	DO-356A/ED203A Compiled Draft distributed to SC-216/WG72
July 24 - 28, 2017	Joint WG72 / SC-216 Plenary Disposition (Hamburg) -> Registration needed
September 12-14, 2017	WG72 Plenary OC Decision Meeting (Toulouse, APSYS)
September 12-14, 2017	SC-216 Plenary FRAC Decision Meeting (DC, RTCA)
October 13, 2017	Draft review completed and comments provided to editor
October 13 – November 3, 2017	Comment resolution in editorial groups
November 03, 2017	Comment resolutions provided to editor
November 13-17 2017	Comment Disposition Meeting (Brussels, EASA/EUROCONTROL)
December 11-15, 2017	DO-356A/ED203A FRAC / OC Decision Meeting (Melbourne/Florida, Embraer)
18. Dec 2017	DO-356A/ED203A FRAC/OC Ready version to RTCA/EUROCAE PM
08. Jan 2018	DO-356A/ED203A Begins FRAC/OC
23. Feb 2018	DO-356A/ED203A FRAC/OC Review Period complete
05. Mar 2018	FRAC/OC Initial disposition by Authors distributed to SC-216 / WG72
19. – 23. Mar 2018	DO-356A/ED203A FRAC / OC Disposition Meeting (Paris, EUROCAE)
29. Mar 2018	DO-356A/ED203A FRAC Comment resolution proposals completed
09. - 13. Apr 2018	Final DO-356A/ED203A FRAC / OC Disposition Meeting (DC, RTCA)
*07. May 2018	DO-356A/ED203A final version to RTCA/EUROCAE PM

* Deadline for RTCA/EUROCAE approval by summer 2018.

Agreement that the group could continue to work on editorial changes for the rest of the meeting

Lunch
Afternoon session editorial changes
Going through editorial / minor comments only as we cannot make a change that will impact the FRAC vote taken before lunch, i.e. filter for editorial, document structure, and terms & definitions (see comments sheet for status and details)
Chains of protection no longer in document, not defined

Use attack paths
SDAL and SEAL no longer used
Change impact analysis – no need for changes at this time, used several times in document
Discussing threat vs. hazard, mean the same in safety, but not security
STPA-SEC glossary – remove
CSD EFB – what does CSD mean? Cockpit situation display
Cleaning up / deleting TBDs – they are all in section F
Inputs from Larry and Dan, save for later
Special thanks to Michel for his hard work as editor of the document!
Adjourn

5. Friday, December 15, 2017 Day Five

About half the in person attendees have already left
Editorial Changes
Editing of TBD's and correcting internal references
Using time to go through editorial comments to reduce the number of editorial comments that come out of FRAC / OC
Also look at inputs from Patrick, Dan & Larry?
Discussed comment on sentence "The event is not the result of an accidental introduction of a vulnerability…"
What is IUEI and what isn't?
Getting away from editorial only, so may need to table this until FRAC
More people are leaving, so adjourning meeting early
Michel will put the finishing touches on document and send it out
Expect bulk of comments to come toward end of FRAC period
FRAC will start January 8, 2018
Happy holidays!
Adjourn

6. Main decisions and actions

Decisions	
Unanimous Consensus from those at meeting and on the telephones to go to FRAC	

Actions	Who	When
Members should continue working on the carried over comments (the non-concur / high put on hold to be “re-submitted” in the review process with fixes. Ideally, these carry over items should have a good resolution proposal within around 30 days (end of January) to get progress and seamless transition to external comments as they come in.	All	January 31, 2018
Renew editorial groups (or focus groups) to carry forward a more efficient approach - what generally worked at the end.	All	
Set up bi-weekly webex sessions starting 9 Jan to work FRAC/OC comments	Karan	Prior to 8 January