EUR 49-17 / WG72-95
RTCA 060-17/SC216-067 Malakoff & Washington, February 23, 2017

Summary of the Plenary Meeting of RTCA Special Committee 216 (Meeting #31) EUROCAE Working Group 72 (Meeting #43) Aeronautical Systems Security

DATE: February 6-10, 2017

PLACE: Honeywell Deer Valley Facility
21111 N. 19th Ave.
Phoenix, Arizona

The Group wishes to thank Honeywell for hosting this meeting.

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

ATTENDEES:

SC-216 Co-Chairs

David Pierce	GE Aviation
Daniel Johnson	Honeywell

SC-216 Secretary

Siobvan Nyikos	Boeing Commercial Airplanes

Designated Federal Official:

Varun Khanna	Federal Aviation Administration (FAA)

RTCA Program Director

Karan Hofmann	RTCA, Inc

Members attended:

Raphael Blaize (APSYS, EADS)
Liz Brandli (FAA)
Claudio Henrique de Castro (Embraer)
Gilles Descargues (Thales Group)
Brode Doorner (Triumph Group)
Patricia Fuilla-Weishaupt (APSYS for Airbus)

Marc Gallant (L-3 Communications)
Marty Gasiorowski (Worldwide Certification Services)
Chris Grant (United Technologies Corporation
Larry Hannert (Aerospace Systems Cyber Security)
Philippe Marquis (Dassault Aviation)
Michel Messerschmidt (Airbus)
Patrick Morrissey (Rockwell Collins)
Bernie Newman (Astronautics Corporation of America)
Ifeolu O. Ogunleye (FAA)
Romuald Salgues (Airbus)
Mike Severson (Bell Helicopter)
Denis Sheridan (Synopsis)
Peter Skaves (FAA)
Brittany Skelton (Boeing)
Mitch Trope (Garmin)
Mohammed Waheed (Aviage System)
Phil Watson (Panasonic)
Doug Young (Gogo)
Scott Ziebarth (Belcan Engineering)

Members attended by phone:

Cheyenne Del Carmen (FAA)
Roman Fischer (Skyguide)
John Flores (FAA)
Raoufou Ganiou (TCCA)
Armelle Gauthe (Airbus)
Clive Goodchild (BAE Systems UK)
Judy Heredia (FAA)
Owen Jing (Department of National Defence of Canada)
Marcus Labay (FAA)
Kevin Meier (Cessna Aircraft Company)
Jean-Paul Moreaux (EASA)
Cecile Morlec (Airbus)
Marie-Chantal Mouret (Airbus)
Ravi Nori (Teledyne Control)
Juri Pauletti (EASA)
John Rankin (MD Helicoptors)
Cyrille Rosay (EASA)
Chuck Royalty (Aerospace Systems Cyber Security)
Shohreh Safarian (FAA)
Stefan Schwindt (GE Aviation)
Stephen Sterling (Department of National Defence of Canada)
Dale Taft (Robinson)
Tim Tinney (Saab Group)
Julien Touzeau (Airbus)
Isidore Venetos (FAA)
Tong Vu (FAA)

Note: Attendance was recorded via the verbal roll-call, the sign-in sheets at the meeting, and the list of people logged into the WebEx. Apologies if anyone was missed.

In accordance with the Federal Advisory Committee Act, Varun Khanna, Federal Aviation Administration (FAA), was the Designated Federal Official.

This meeting consisted of both plenary and working sessions.

The outline for this meeting summary is organized around the published agenda. SC-216 presentations and documents can be found at the committee's Workspace site at http://workspace.rtca.org . Please contact the Program Director for access to the site.

Details of document edits are generally incorporated by reference in this summary. The agenda was published in advance of the meeting, and is available from the RTCA website.

Meeting Summary

Day 1

Varun Khanna: Public meeting announcement:
In accordance with the Federal Advisory Committee Act, this Advisory Committee meeting is open to the public. Notice of the meeting was published in the Federal Register on January 10, 2017. Attendance is open to the interested public. With the approval of the Chairs, members of the public may present oral or written statements. Persons wishing to present or obtain information should coordinate with the RTCA Program Director Karan Hofmann and Chairs David Pierce and Daniel Johnson.

Karan Hofmann: RTCA and EUROCAE proprietary references policy:
RTCA seeks to develop standards that don't require proprietary information for compliance. However, patented technology and copyrighted material that are required for compliance may be included in a standard if RTCA determines it provides significant benefit. If your company holds a patent or copyright relevant to an SC-216/WG-72 document being developed, advise Karan Hofmann, Anna vonGroote, Dan Johnson, Michel Messerschmidt, and Dave Pierce.

Karan Hofmann: RTCA and EUROCAE membership policy:
Organizations with a representative participating on joint RTCA Committees and EUROCAE Working Groups must be members of RTCA or EUROCAE.

The Chair Dave Pierce opened the meeting and introductions were made around the room. The agenda was reviewed, and the minutes of the last meeting were accepted.

Cyrille Rosay gave presentation addressing what if harmonization cannot be achieved and the implications

3 scenarios with DO-356A and ED-203A:

- ED 203 and DO- 356 propose a unique method

- ED-203 and DO-356 are identical but proposing 2 different methods A and B
- ED-203 and DO-356 are different in methodology: ED-203 proposes method A and DO-356 method B

4 scenarios with authorities:

1. FAA recognizes method A only and EASA method B only, or
2. FAA accept DO-356 and EASA accepts ED-203. As docs are equal both methods are accepted
3. FAA recognizes DO-356 only, EASA ED-203 only
4. FAA and EASA recognize Both DO-356 and ED-203 as acceptable means.

Varun – not acceptable for applicant to be on the hook to do both methods, give them an objective and if they meet the objective with whatever compliance method it should be accepted, prescriptive method is asking for trouble, FAA in favor of supplier decides which method he wants to apply

Philippe - have in the document something that can help to compare the 2 methods

Bernie – during ARAC, both cert authorities would recognize both approaches as equally acceptable

Dave – if you meet the risk acceptability matrix, it shouldn't matter what method, you can revisit if needed, this is where everything in the aircraft comes together

Dan – a lot of artifacts between the two methods are common

Michel – one process defined in documents, can have different implementations, still needs to be compatibility

Dan – two questions

1. When we evaluation risk, what is the evaluation criteria?
2. How complete is the assurance? Do we want a complete or supplemental list? No conflict, just how we put it in the process

Philippe - Can discuss later, not agreement on what is complete vs. supplement, concern about content as opposed to presentation, what is the basis of the data package

The activities themselves are common, what is different is the way it is implemented

Michel - both methods shall/can be acceptable

Dan - need to agree that both methods cover the same objectives but do it in a different way

Michel - need to have something that is usable on both sides

FAA status of ARAC (Varun):

Resource limitations will drive prioritization of recommendations, marching orders for SC-216 are the same, put ARAC report recommendations into guidance material, do not want functionality creep or to reopen DO-355, need milestones to show progress after every meeting, TOR for SC-216 and WG-72 need to agree

Peter – plan to send updated ARAC recommendations and priorities to industry and EASA, regarding rulemaking, the only chance is to start with part 25, if we address all at the same time it won't be possibility, especially with changed administration, waiting on interpretation of executive orders, hiring freeze for federal employees

Schedule discussion (updated schedule will be posted)

- March Brussels meeting, need confirmation of host / meeting site from Stefan, EUROCONTROL
- May meeting will still be in Washington, DC due to time zone for virtual participants in Europe
- July Hamburg meeting, Michel to confirm Airbus will host

Action item review (Michel), see master spreadsheet for details

Need a new person to the group and DO-356/ED-203 to volunteer for 3.2 introduction to risk management, Marty volunteered

Varun - Haven't talked about rulemaking changes in part 21, security organizations, certification of personnel, etc. Can't be dictating this, if you meet the objectives, you're good

Mike – purposely took language out to prevent companies being forced to put in organizations, nothing on the safety side about training for these positions

Lunch break

Review of WP Section 1 – Dan Johnson, scope statement

Peter – if someone wants to use the document, tailor the document, etc. they should be able to, but don't need to follow line by line

Dan – developed with part 25 in mind
Mention of CS25, part 25 seems to be a problem for some people
Importance of terminology/definition
1.5 - need to add reference to ED204 to be kept in mind for the future
WP can be closed

Review of WP Section 6.2 – Romuald Salgues, logging

ARINC 852 standards for logs, don't want to have more than one standard/format, standard still being written

Phil - Concern if you go to ACD, need ARINC to approve standard

Michel - Written for commercial but could be used for ACD

John Flores – left it up to DAH, ANSOG has info about logging, what to do, 90 day retention, etc.
Dan – don't need to go into specifics here, but do need to for the ANSOG

Marty – why log successful attempts?

Dan and Michel – possible that a successful attempt is a successful unauthorized attempt or attack

Discussing "Maintain product security" figure again, edit or remove?
2.1.2.1 - Need to update the figure which comes from an Airbus document (action to Michel)

Replace product security by continuing Airworthiness (changes and events)

ConOps #3 modified

Romuald - Section 2.1.2.3 is purely a US concern, "…records may contain evidence of unlawful activity…" (wording Chuck suggested)
Dan – we were trying to avoid this because every country has its own laws
Decision – delete section, proposal not accepted and removed. No added value from this information

Marty – why is paragraph on special conditions in here? (Brittany's concern as well)

Varun and Michel – only vehicle for implementation requirement for 90 day retention
Will revisit when there is a rule to replace special conditions, but won't happen anytime soon
Varun – actually, Stefan is right, it's in the MoC (ANSOG), not the special conditions

Pilot needs to know what failed, not why it failed
Ground cares about why it failed

2.2 - Proposal to replace systematically by consistently is not agreed - 1st sentence modified
Event logging is implemented only to answer authorities' request
Note OK

ConOps#4 modified and agreed
2.3 - Title modified
First sentence modified (rephrase)

ISO (Airbus term) is replaced by "reportable event or service difficulty"
2.4 moved to 2.3.1 regarding the note discussion on TSO holders being able to act as DAH
Roles:

- TSO holder provides instructions to STC holder
- STC holder implements instructions
- Security events to be logged are defined by the DAH

Varun – responsibility should be with the TSO who builds the box

Consider changing CONOPS to other structure
ConOps#8 generally removed

Action ED-204 should be added everywhere with DO-355
2.3.2 ConOps#10 modified and agreed

ConOps#11 modified but not to be kept as a ConOps (Objective for example)

3 working papers on architecture -> skip to risk acceptability discussion

Review of WP Section 2.7 – Bernie N/Dan J/Michel M

Ties to section 3.6

Michel – OK with likelihood as long as not linked to probability, like 1309
Reviewed proposed definitions before using them in paper
Reviewed proposed combined risk assessment matrix

1.4 - Stefan concern about the table
Philippe, think about how we use likelihood for assessment
Level of threat is not yet assumed but try to do the exercise

Issue with term “nominal”, doesn’t translate well

2.7.1.3 Level of threat
Table 2 to be split in 2 to avoid to put safety effect in relation to SDAL and avoid this table in the final document
Objective is not to agree on the full paper but to agree on the direction to be taken
Discussion to decide if Common risk acceptability can be agreed despite 2 different methods for risk assessment

Michel asks if a low likelihood is the same as a high effectiveness

Assessment at aircraft level when systems has been assessed with the other method? Hybrid method won’t be accepted by authorities

2.7.4 Discussion about security that evolves with time
Action 2.7.4 to rework to avoid misunderstanding

As a conclusion, provide comments on this WP
Barriers with agreeing on this paper today - Romuald wants to reserve the right to retract and fix issues that are discovered after these meetings
Dan – concern is to collect comments made along the way
Concern that this is “kicking the can down the road”, not our intention

This is about risk acceptability, part of document at the beginning

Philippe - We spent so many time on this subject that splitting it into two topics was a way of moving forward

Larry – originally chapter 2 was supposed to be this from the regulator’s perspective, and other perspectives were in chapter 3

3.6 – there is a lot proposed text in ARAC report for likelihood, level of threat effectiveness

Dan – 201 allows different risk assessments between organizations as long as there is effective communication
Dave – communication only happens at a few points
Dan – need compatibility of risk assessment, not identical
Dave – table should be fine, don't need to go deeper

Going back to whether we can have both methods or still need to harmonize on a method
Cyrille's presentation from earlier - presented some options, some not acceptable to committee members
Dan – want something that works now and later, not something that works only at one point in time (referring to ease-of-execution likelihood)

Day 2

Rotorcraft discussion:

Liz Brandli (FAA) – no issue with rulemaking language, issue with MOC, didn't have enough rotorcraft rep, leave part 27 and 29 out of scoping language, Dan removed that language, right now looking through best practices document, we are open to an applicant using the three ED/DO documents and tailoring for rotorcraft, but would prefer to look at best practices for cyber security for rotorcraft

Mike Severson (Bell) – concurs with what Liz said about ARAC, Gama safety related process

Varun – exposure window and flight duration is different from normal part 25 airplanes, therefore we believe we can handle the security for rotorcraft through other means being used today, up to rotorcraft whether they want to enhance that via AC or other means

Peter – if you look at safety risk management, we wrote first Special Condition (SC) on 787 10 years ago, write rules every year, we have yet to write one on security, have not written an SC for rotorcraft (Liz confirmed), during ARAC developed a policy statement on when SC applies to different FAR parts, can EASA do something similar but different, want to harmonize on when SC apply

Airbus Helicopter - follow ED-203 publication with impact

Liz – issued one IP on Bell using 1309, has not seen SC, IP, or MOC from EASA on rotorcraft

Julien – discuss EASA position with applicant and share with the FAA, want to add specifics about rotorcraft

Romuald – put an appendix in the document to deal with rotorcraft, is this an acceptable approach? Yes

Need for creation of a tailored approach for rotorcraft harmonized for all rotorcraft manufacturers and not only for Airbus
Liz – need more involvement from community if Airbus puts language in documents

Varun – Airbus can use documents, but that doesn't mean rest of rotorcraft needs to use them, don't want this to be mandatory

Mike – use safety processes but make sure security functions are addressed, working with FAA to set positions, not planning to use DO documents

Dave - ASTM document being built to same comment
Patrick - Gama sent to ASTM for validating, intended to be more lightweight

Stefan - 1309 has been tailored to apply to other parts
Dale – stay with 1309 safety assessment, small helicopters that don't have fly by wire controls, not same scope that document have been constructed for

During ARAC, some time spent to provide recommendations for rotorcrafts
Bernie – was ARAC recommendation enough to work from?
Romuald – recommendation from ARAC report to put rotorcraft language in tailoring in
Liz – we did not agree with that recommendation, not enough representation from rotorcraft in ARAC

Ifeolu Ogunleye – two recommendations as MOC, are we going to change the DO document or use best practices?
Solution – the applicant has the option to use either the DO/ED document or the ASTM document, how does EASA feel?
Marty – there are small things you can do to DO-178 to apply to rotorcraft
Varun – that's what ASTM is doing

Shohreh – rotorcraft exposure times increasing, example is on an oil rig

Summarizing…

Fundamentally, FAA does not want to use DO documents for rotorcraft, however if applicant wishes to use, acceptable as long as it is not mandatory

EASA and Airbus want to tailor DO and ED documents in the appendix so that the documents still apply but appendix says do something different for part 29 (nothing about part 27)
ARAC wants to revise rulemaking for part 27

Mike – don't want a new rule, but wants to be involved in developing language if there is a new rule

Varun – put out an AC

Ifeolu – Are we opening all three? No. Will tailoring the one (DO-356) be sufficient?

Dan – not scope of committee to organize discussions and come up with language

Dave – not action to committee, action to rotorcraft community

Group to be organized for rotorcrafts - Stefan will organize a meeting, send names to Liz and Stefan

Should start with discussion of ASTM document

Long story short – SC-216 and WG-72 aren't going to create working paper or discuss language to put into an appendix. Liz and Stefan will set up their own subgroup with the rotorcraft community, come up with the appropriate language, and then give to us to incorporate into an appendix, assuming that direction still stands.

Review of WP Section 4 Supplemental Approach – Dan J/Michel M

Not much has changed from last time reviewed, reviewing comments spreadsheet (see spreadsheet for details)

Supplemental vs. independence
Independence does not take into account safety
Michel confidence in security and need to agree on activities for security

Dan – still want to due process on malware
Pat – Static analysis of code for vulnerabilities not the same as looking for malware, own more of the supply chain if you are compiling the source code yourself
Dan – correct, intent of this is malware
Chuck – only for procured software developed with assurance objectives, clarity would help, hazard is reduced because architecture of system that incorporates software helps mitigate

Intended function
The only thing we test for at level D and E (really just D) is intended function, from that perspective, if malware or vulnerability, in COTS compiled or source code, we don't have access to source code
If we have access, there are things we can do about it
Certain additional things depending on case
Varun - Source code review – need to be careful, don't want to change objectives for level D
Marty – you can take Linux or windows version you want to use, but an auditor might ask to qualify virus scanner (however, not at level D)
Decision - Scanning should be an activity, the objective would be the detection of unintended functions, action to Dan to modify the document to put scanning as an activity and modify the objective
Keep different from source code examination

Development and production tools should be covered under the baseline program
DO-330?
Looking at tables, system development process assumptions
Which supplemental objectives apply to your system? Dan used A+ SCC, B+ SCC, etc.
Dan – DO-326A talks about assignment of assurance objective, defines security and assurance requirements for systems, subsystems, and items
Philippe – assign security measures

Pat – emerging isolation capabilities
Chuck – isolations techniques, if good for security, should be good for safety, need FAA and EASA to weigh in
Michel – not necessarily true
Goes back to US vs. Europe view of safety & security

Need to partition SW – isolation is good for safety

Supplemental approach only applies when DAL and security level are compliant, if not use the independent approach
Most cases are for low safety levels and high security levels -> this method won't be applied a lot
Combine 2 approaches
Supplemental approach only to address specific cases, so is it still relevant to keep supplemental approach?
For ground system, need for independent approach but are not in the scope of this working group
Philippe – many examples of implementation to put security control in low DAL box

Dan - Need clarification on what other objectives WG-72 wants if we want to implement in document
Michel – need to evaluate and analyze different implementations, unintended behavior
Bernie – we identified one additional objective, malware

Dave – more emphasis on talent of security team rather than process, if you don't catch something, it's not the fault of your process, it's the fault of your team or not having the right people on your team
Marty – if you don't have people with domain experience, you're going to miss requirements, during test you'll discover missing requirements, ARP process and supplemental process -> we have enough

Lunch break

Continuation of Chapter 4

Discussion of preliminary assessment
Dan – don't see submitting something preliminary to the cert authorities if the design is inadequate, cert evidence needs
Michel – preliminary might not be acceptable yet
Claudio - Left side of V, design not acceptable yet, learn more as you go up the right side of V, found something but not solution
Dan – purpose of preliminary is to show that intended design is secure
Varun & Ifeolu – want to at least see a plan, if there is an anomaly or finding, want to see a plan for how to fix or approach it
Ifeolu – when does your preliminary become final?
Varun – if authorities see risk is not acceptable, they will reject doc
Denis - If risks in prelim are always acceptable, you never go to bottom part of figure 2-1 from DO-326A, security development related activities
Ifeolu - analysis is performed
Philippe - Prelim is what you perform during design, final is what you perform on real finished product
Decision – change to preliminary system security assessment risks are performed (replace "acceptable" with "performed")

Dave – this table is the security supplement to safety, if the row is in safety, it should be here too
Continue comments spreadsheet (see spreadsheet for additional detail)
Discuss STC table in STC section 2.3

Dave – solution should be in independent table

Varun reiterated FAA position on controls on DAL E, don't care about DAL E system as long as it doesn't catch on fire

Phil - How can you take credit if it can take place without certification review, what if there is a new software version the next month?
Varun - As the applicant, you are responsible for ensuring controls are functioning
Don't want IFE systems to have to bump up to DAL D
Put up ARAC report, not much resolution, minimal consideration is paid to DAL E systems, if implemented and verified to function as intended, can provide layer of security, must be commensurate with level of threat
Chuck and Varun – example where loss of system does not result in a hazard, adding a wifi access point to an installed system, DAL E, add controls to it
Peter – if you need security controls on a sys that has no safety effect, how can it be Level E? Nothing matters vs. Level D
Dan – discussion of software only level D so you don't need to go through hardware aspects

Michel - IDS, IPS, can use on aircraft but only useful if you can update signature immediately, won't work for operators

Chuck - Incorrectly assigned if alternation to software can cause an effect
Example to consider – wifi access that allows maintenance access, put security control, no impact if it fails, would leak info that the regulators and airlines don't want public to have access to, DAL E as there is no effect, still care from security standpoint
Gain access to more functions at higher criticality
Phil – demonstrate, but can't take cert credit

Discussion about various kind of assurance:
Product assurance -> the right product?
ARP/DO -> good process, not the right product

Presentation of figure of assurance categories
We need to know what we want to do before trying to classify types of assurance
Need to reconsider the classification
Philippe – correctness will be checked at higher level, but in terms of evidence, it will be provided through security assurance requirements, not safety assurance requirements

Consider more than failure, consider if someone can authenticate
Michel – what if system isn't stable enough and crashes, reboots, etc. Process of access control crashes or reboots and allows for connection

SCC for DAL E -> discussion to explain why we can have a need of security even for an equipment with no safety impact, as attack can propagate to safety related items
Change tables so that DAL E security measures are only handled by the independent approach

Process for dealing with derived requirements and security requirements is the same as with all requirements

Finished going through comments spreadsheet

Review of WP Section 4.8.2 – Chuck Royalty

Philippe questioned definition of assurance, 1.3.1. In 2nd part of the sentence, need to take into account security (adding free of vulnerability for example)
Effectiveness assurance vs. development assurance, should have the same considerations, Chuck did not differentiate between the two in his paper

Working through example in figure 2-3 annotated security architecture, Threat condition should be used when there is a safety impact

Discussed exposure and assurance section, background, not part of paper, Chuck wanted to raise a separate but relevant issue with latent failures
Discussion on the need to use method for establishing exposure time of a security measure and having a detection mechanism
Varun - Do this check before dispatch? Pre-flight check on primary flight controls computer good enough?
Chuck - If security folded in, yes that's the goal. Can envision systems and architectures that won't allow that to happen
Varun - Security is protective function, not the function
Dan – detectability is a concern

Day 3

Review WP Section 2.5 Continued Effectiveness – Dan Johnson

ARAC wants us to do gap analysis between DO-355 and other material
Dan hasn't incorporated Boeing material yet

Fail secure concept is used at Airbus (when security protection fails, no way to get in)
Log mechanism does not allow reacting immediately

Gap analysis (see WP for complete list):
Need guidance from Security Management System
ER-013 security glossary, Dan would prefer that the glossary itself be updated
Continued airworthiness security process specification, ARAC recommended FAA establish policy to leverage existing COS, there is proposed text in WP
AC 119 talks about digital signing, but DO-355 does not require it -> regulatory issue, DAH can require it
Control of aircraft conformity to type design – this needs to be discussed
DO-355 discusses how you use security environment, but does not discuss how to manage it, content controlled by DAH, currently no guidance on how operator manages security environment (Is this true? See ANSOG)

Marty – installed dataloader that performs security function can be dispatched, different from a security function protecting from the IFES
Pat – if system fails closed, we don't care

Varun - If protective mechanism fails but does not affect system, we have issue. Currently no one is going to say dispatch

Dan - If equipment is in IMEL list…as we put security features, does that affect IMEL?
John Flores – from IMEL perspective, airplane safer if LRUs working, recently probably with Alaska and United using IMEL because they had late delivery not able to get ANSP approved in time, ONS, violation, nothing wrong with ONS, just that they didn't get approved in time to load software, not allowed to use ONS, went to Boeing and Honeywell and removed/replaced as they would a normal LRU
No effect on continued operation

Overall architecture, if system itself indicates issue through ICAS, nothing to do with security, benign to crew
Peter – avionics have health monitoring, if algorithms looking at security, affecting LRU performance is one thing, depends on how it is designed
Romuald – if security protection and no way to penetrate…
Chuck – not unconditional that if a security control fails it causes ICAS messages, use dataload as example, solution works only if you are assured that the ONS in absence of ANSP cannot load airplane on its own, be loaded by an attacker

John – policy and procedures, aircraft has to be type design, proven and controlled, FAA has policy and procedures, so no gap re: #2 under gap analysis, don't need to put something additional in DO-355, already understood

Look at proposed text
Insecure condition should be replaced.
Objective: define what needs to be in the security guidance

2.1.2 Need to monitor protective functions and inform crew if something needs to be done

2.1.5 Added value of this paragraph as it is the same as TC holder. The 2 chapters could be merged
Security content for MMEL
Varun - Systems on MMEL are responsible for integrity of their own load, unless you have message on ICAS saying otherwise, you can't make that determination
Dan – should we remove section or change title as it might not be appropriate
Varun - Not suggesting adding a crew announcement, saying you can't do this without crew announcement, so take it out, Romuald agrees

Dave – need to fail safe, not secure
Marty - if you are going to have a latent failure of security component, what is FHA?
Varun - protective function, not governing function, can fix it, has not failed airplane function, go fix maintenance function

Michel - No different in operator guidance between DAH and STC, DAH includes STC
2.2 Last paragraph before Incident management to be put at the beginning of the chapter

Incident management -> remove the must
Difficulty to get the information and find the right authority to report
Need to receive incident only if they can have a safety effect

Action Dan: ensure consistence with WP on incidents presented by Romuald
Discussion on the need to put the organizations that should be informed (A-ISAC for example) as they are specific to countries
Consistency with DO-355?

Alerts should be analyzed when received
Action to Dan - Need to precise what is relevant information and is to be shared
Siobvan – "Receive reports…" What does Boeing receive vs. what does the airline keep to themselves? How is this vetted? At discretion of airlines. Will propose better wording to reflect what actually happens

Raphael – Change "must" to "should" or something else to fix these
Last bullet re: A-ISAC, NSA, DHS
Dave – remove NSA
Michel – put equivalent for EA-ISAC in Europe and other regional organizations
Phil - Airbus is a member in A-ISAC
Michel - Yes, but even as a member we do not receive all relevant information due to "US eyes only" classifications. Both EA-ISAC in Europe and A-ISAC in US are already in place and should be considered here.

Vulnerability and threat management
Again, remove "must"
Dan – can we trust A-ISAC to send us reports?
Dave – no, A-ISAC is not enough
Phil – they don't send reports
Michel – there are a lot of information flows, not everything is beneficial, what is relevant
Dan – agree that there should be a filter or gate
Michel – don't want there to be a noncompliance because you didn't read a newsletter, but need help vetting what is relevant
Siobvan – do you still plan to incorporate possible security log entries? (Remark from Boeing: Other areas than DO-355 need to be added to this document)
Dan – yes, from ANSOG

Review of WP Section 4 Independent Approach – Dan J/Michel M

Security development and effectiveness assurance merged as difficult to draw a line between the 2 types but can change.-> This is explained in a separate paper
Philippe – should include considerations about distinction between development assurance and security effectiveness
Security behavior = effectiveness

Refutation previously called "security evaluation" inside Airbus
"Refutation tests are conducted for all applicable threat scenarios"
Regarding using ED-202 terminology, 2 possibilities reuse the terminology defined in order that people are not lost. If better terms are now to be used, ED-202 shall be updated
Varun – can we use different word than refutation? not commonly used in US
Patricia - Take action to review structure of doc, compare to ED-202, look at definition, numbering of objectives will be reworked at the end

“Security Assurance Level (SAL) is a measures…”
Philippe – is it a measure?
4.1.8.1 - First sentence SAL is not a measure -> find a better term (indication, means of compliance for confidence)

Discussion around SAL levels
When is SAL assigned in the process? -> linked to risk acceptability
Levels determine how much you need to do to be confident
Philippe - If item is a victim of attack, there needs to be minimal assurance, would likelihood be reduced
Michel - Protect self, not something else behind it.
Dan - robustness in target is a security measure in a target. If you implement a security requirement, that is a security measures
Philippe – difference between security function and measure, would that work?
Dan and Michel – no, then you need to define security function

Reviewing table on minimum security assurance level assignment
Pat - Allows for multiple security measures along attack path to an asset
Michel - Shouldn’t be too prescriptive or architecture specific, need to enforce that there are at least two security measures, especial if there is a catastrophic event
Bernie – don’t want to get into situation where we are unnecessarily prescriptive, DO-178, there is a consideration of the possibility to lower level when you have additional safety monitors shown to be independent, doesn’t say how much to lower

Looking at security assessment activities, tables at back give more info
4.1.9 does not show the way effectiveness is to be dealt with -> need to rely on security architecture
Action - This chapter need to be reworked to explain better the way SAL is allocated

4.1.2 - O2.8 Change proposal: is addressed as needed
Comment: Be careful with the use of various processes, keep the same as in ED-202
Risk assessment, risk management processes are defined but planning process is not

4.1.2.2 - What is important is to verify if objectives and activities are accurate?
Action: Add an explanation or an explicit objective to explain what is complete and validated
Association of activities and objectives are done in tables in annex

4.1.2.3 - Distinguish objectives specific for security from others
Control categories should be considered also

4.1.3.3 - O5.3 is challenged
Need to define the level of granularity the SAL is assigned -> security item
Security architecture should also be renamed, as it does not present only security elements
Need to discuss this paragraph in another place
Opportunity to deal with vulnerabilities in this chapter, to be considered
Big discussion around the need to recall here all activities/objectives which leads to re-explain the philosophy of the approach (specific security activities + activities also done DO but not all activities as they are not all useful)

DO-178 purpose is not safety but avoiding the defects

Common criteria also considered in this way to deal with security assurance
Chuck – concerned about objectives crossing over into other areas like configuration management
Bernie – doesn't want us to end up in silos where there is a silo for security, silo for configuration management, etc. Wording can be more explicit to say some of these activities could be met via ARP, DO-178. Which objectives may or may not be?
For example, PSecAC does not have to be a PSecAC doc, can be handled via cert plan (agree, in 2.4 cert evidence WP)

Lunch break

Review of WP Section 4 Independent Approach (continued)
Michel – won't complete discussion on any of the sections today, but want to make sure we touch all the sections

Varun - Long list of items become default list, only list the ones that pertain to security

Removed process assurance objectives

Steve - Control categories belong in objectives, don't want to contradict ourselves, referred back to configuration control discussion from earlier

Dan - Don't need full change or problem report history, reasons why some artifacts are in one category and not the other

Bernie – Back to previous point, if you follow it via another standard, great. If not, need to do the cc
Dan - Software architecture needs to be well defined, otherwise we don't know when to stop
Peter - In ARP, they talked about hardware and software items, what does it mean, software means DO-178, hardware talking about 254, system interface to those hardware and software items and their respective documents. Security items is a brand new term not in those existing docs
Dan - 178, DAL applied uniformly to entire item, partitioning applied before and determines item
Marty – item is either software or hardware, in other doc it talks about modules which can be HW, SW, or both. For security, you define what the item is and whether it is HW, SW, or both. Up to developer to define their item

Need another term now – subsystem, security item, security function, etc.

Looking at implementation process objectives
4.1.4.1 - Vulnerability dossier not mentioned in this chapter

4.1.4.2 - testing for negative requirement
Terms: negative security requirements, functional security requirements, new term needed? Functional implies functional testing and you get into the issue of positive vs. negative
Refutation is not yet defined in glossary
Stop criteria still need to be defined
Need to explain more what is refutation and why it is needed -> presentation to prepare for next webex?

Peter - We have been discussing process specs, no requirements for avionics system but requirements for modifying documents? Does not make sense

One standard to address system, software, and hardware
Supplemental is trying to do that too
All part of the baseline program
Peter – Use existing processes, why need supplemental?
Michel – Want to feed into existing processes, but it assumes we are all following the same processes, which we are not. Companies want to find their own way
Dan – there is a group of people (subset of WG-72) need set of security objectives that are objective and don't depend on 178, want security people to be independent org
Varun – don't impose it on everyone else
Stefan – ARP 4754 is not applied to engine propellers, 178 we also have question of versions

Patricia - Security assurance based on security activities, need to take credit, if DAL C or higher don't need to do the activities listed, a lot of activities but not all the them
Liz – partition is critical
Larry – makes sense when you're writing the code, but a lot of this is being applied to code that is already written, get as much out of process as you can, knowing that you can't go into DO-178 process and start from scratch
Varun – never be able to patch security in, intrinsic to system
Larry – yes, but if code already written, DO-178 is helpful
Varun - Windows in level C boxes today, assume it will fail and ensure your architecture can deal with the failure, that is how you do it without partitions
Michel – is it useful to do DAL D on a dataloader?
Dave – if you use it on a DAL A system, it depends on whether the DAL A system has its own security, if not or it's not sufficient, dataload does need to be at DAL D
Chris – DAL A system needs to protect itself regardless. We are chasing levels of security by tying to DO-178 levels (agree)
Chuck - Can't control attacker, can only control product, so develop product with worst case in mind

Varun – what is the definition of refutation?
Michel - Refutation confirms your requirement has been implemented correctly, usually requirements stated in positive way so you can verify them, refutation testing includes negative testing and penetration testing as well
Dan - May be source of new requirements and validation

Review of Appendix Security Example – Claudio C

Example of an aircraft and architecture that does not exist, use example to put through harmonized methodology and ensure it works
Phil – issue with failure analysis at end of table, why minor impact on loss of connectivity on IFE?
Claudio – because it's connected to other functions, crew
Phil – tell crew to power off system if anything bad happens

Aircraft airworthiness security process example
Example is filled and ends with the definition of the scope and environment
Remains to do all other activities (risk analysis, architecture, etc.)

Good to understand of how everything works and people can join to go on with the development of this example

Michel – would like to add example to appendix and apply methods and processes to this example to ensure they would work in practice, a lot of work but everyone can pitch in, good opportunity especially for newer members

Team dinner at Claim Jumper

Day 4

Review of WP Section 3.1 – David P/Cecile M/Claudio C (security scope)

Going through comments sheet

Scope considers all levels (Aircraft but also system and sub-systems)
Dan - Not a system level, several system levels, hierarchy of systems
Stefan - Need to perform activities on LRUs as well, LRUs may have subsystems within

New action to review doc for AEH and SW, may need to propagate to that level
Philippe – why are there three parts to security scope instead of original two?
Michel - All three parts in security scope in 202A, just not stated as a separate bullet point

Intended accessibility
Dan – change to accessibility requirements, what is accessible to whom, if our security environment says the cockpit is accessible, what can we do, it's more likely that we will say the cockpit is not accessible in environment. At what point do we determine what is and what is not accessible?
Stefan - Cargo aircraft, cockpit is inaccessible to the few passengers
Passengers can be crew, couriers, or supernumeraries
Part of trustworthiness assumptions

Discussions around trustworthiness
Need to inform design of what is trusted or not and to document it
Dan - In cargo planes, do we have standing physical security assumptions? If so, include them in security environment, suggestion to discuss during trustworthiness section, don't need to decide now
Michel - Zones – define rules and organizations
Stefan - Cabin information systems in passenger area, passenger technically has access
Dan - Non trusted zone needs extra protections so it's covered
Dave – taking the word "intended" out per comment

Take out "list of possible attacks through the points of entry", does not belong in this discussion, also it is identification of possible attacks rather than list
Overall comment – replace "list" with "identification"

Included discussion of attributes Confidentiality, Integrity, and Availability
Pat - Only part of document that talks about properties of assets, critical to asset discussion, are you affecting part of asset that is critical? Should move this discussion up to asset section

Claudio new comment – remove text added by previous comment and fit into 3.1.3, change section title to Threat Source Characterization

Dan - If we discuss trustworthiness, needs to be trustworthiness assumptions, documented and negotiated with authorities, not have guidance on when and when not to trust something, separate working paper
Michel – WG-72 does not have a proposal on trustworthiness so far

Level of threat is associated to the threat source, need to characterize the threat source in the environment
Dan makes a new proposal for 3.1.3. Cecile to participate?
Philippe – strange for someone who doesn't understand the problem to read this, why associate level of danger with threat source? Reference when we speak about threat scenario as level of threat assessment when you assess threat scenario, associate to characterization
Michel – can argue it's not useful
Romuald agreed with Philippe
Michel – have called it attacker profile
Dan – whatever info you need about threat source to do risk assessment
Population isn't trusted vs. not, need to consider classification of assets

Request to retitle 3.1.5, need clarify layers re: LRUs and subsystems, need title to reflect that issue

End of comments, see comments spreadsheet for more details

Already started touching on trustworthiness discussion
Cecile has action to get feedback from Airbus and WG-72 re: trustworthiness, look at ARAC report, provide inputs, can even incorporate into existing paper

Review of WP Section 2.4 – Siobvan Nyikos

Uses GM7 from ARAC report

What is important is to have document or data to be mapped with 1st column (DO-326A Table 4-1 list), required data can be mapped into whatever document(s) you wish, does not need to be an even one-to-one

Certification evidence are the documents shown to the Authorities (MoC). All other data are substantiation data. Distinction to be made in this document

At what level are you required to submit this data, aircraft or system?
- Not at item level
- if you have an add-on product, that will be a "system" in this context
- Siobvan to add aircraft/system paragraph discussing this

"Conditional for change" highlighted in yellow means that these documents are to be updated only when needed and requested

STC needs SSIG as input to ANSOG
- OEMs had a problem with this idea; it is not submitted to regulator
- We have another paper discussing this (2.3)
- Question: Is SSIG to be kept as it is related to design process and not certification? (Claudio)

Summary of Actions for proposed text:

- Differentiate between compliance data and supplemental data when you are talking certification evidence / data (Philippe)
- What is required for system vs. aircraft? Consider if we need to include text to address Stefan's concern, or will that be covered in the STC section?
- Change text for "conditional change" to "dependent on certification project" (or something else)
- Explain why it's conditional, use example of how ANSOG only needs to be updated if the change or project drives a change to operator guidance (Shohreh)
- Don't include SSIG in ASOG, discussion on whether or not appropriate to include Integrator Guidance (might need further clarification)

An update of the document will be provided for next meeting

Review of WP Section 2.2 – Gilles D/David P/Romuald S

Gilles presenting

Section 3.1 also deals with assets

A Classification major and above are allocated after risk analysis regarding security.
Already discussed during ARAC -> keep only the classification regarding safety and other cases are addressed by the examination of propagation to other systems (see paragraph at the end of document)

Dan – break into two parts

1. One part talks about Major/Minor changes
2. Second part COTS, discuss separately (need clarification, Major/Minor changes re: DAL or re: determinations)

A minor asset can be a way to propagate to another system (major or higher)

Don't include ARAC examples

Peter – AC coming out to clarify this, however too many regulations already, 3000-4000 emergency ACs, need to arrive at 90-95% solution, companies trying to implement best practices

Dave - Minor, not connected or ready only – should be easy

The final list of 4 bullets is not exhaustive but all cases mentioned are always true -> Introduction sentence could be reworded
The cases that are not in this list need to be evaluated

Move primary assets consideration in 3.1
List things that aren't so easy

Need to consider internal and external threats (also includes COTS, FLS, etc.) -> no as it increases what authorities request from applicants.
Michel – why specify between COTS and non-COTS?

Dan - Includes COTS guidance material not here but elsewhere in guidance doc, a lot of this is from old material, action to include material from 4.3 ARAC report in document

Also removal of domain considerations in discussion (Romuald), no need to consider domain regarding protection of assets-> list in 2.2.2 will be removed

Michel – your understanding of ACD might be different from another manufacturer or supplier
Dave – Ok with removing domain references

Lunch break

Review of WP Section 2.3 – Romuald Salgues/Siobvan Nyikos

Romuald presenting first, ARAC report wording is used in this paper

Objective: STC does not compromise certification gained by TC holder

2.3.1 should be simplified

Pat - Does decision need to be obtained from OEM re: if STC outside security perimeter? OEM Classify modification per security impact

Romuald and Siobvan discussing again whether examples of major criteria should be included in this proposed text, Romuald believes we can still include without disclosing proprietary info
(Use Claudio's aircraft architecture example as litmus test?)
Major and Minor are not considered in the same way by Airbus and Boeing -> better not to put examples but base it on objectives. Criteria for classification of changes is not yet defined. For now, classification is just agreed between applicant and authority for each change.
Philippe - Don't want to stick on another regulation like Part 21
Stefan insists that we need examples
Dave reiterated that neither Boeing nor Airbus want to disclose, even a "watered down" version

Stefan – don't want to repeat activities, in Europe makes a difference on who can certify, EASA has only three people who can do security right now
Airbus minor – use delegation
Airbus major – go to EASA

Peter – use other documentation to address part 21

Propose take out 2.3.3 Services Tree section, no one knows what it is

Phil - Change "single" to "every", don't italicize, 2.3 "prior to a single modification" to be replaced by "prior to every modification"

Shohreh wants minor aspects included in change impact
Romuald – change impact analysis already includes both major and minor, what is the concern?
Dave – this detail would be appropriate in another section, not here
Should we include proposed text?
Michel – keep text

2.3.2 – link security to general impact analysis, keep first paragraph, not looking at another change impact analysis for security, looking at general and linking to security

This WP will be kept for further discussions with authorities but is not to be included in ED-203 completely, only STC part should remain in ED-203A.
Need for ED-203 is to add what can help to clarify ED-202A

Review White Paper on Security Audits – Romuald/Shohreh/Stefan

Peter – this does not belong in this process, you can present a whitepaper to the authorities, but that's it, not part of ARAC or committees
Michel: value for WG but low priority as it won't be in ED203
Presentation of document - Security assurance audits are to be performed independently of audits performed in relation do DO-178 and DO-254

Liz - Removed SOI guidance from orders, looking for more process based approvals, things are changing, removing stages of involvement
Stefan – one option is to take existing audit and through security in, other option is have a completely different audit for security
Recommendation depends on who you ask

Next topic - vehicles for communicating security to authorities and auditors

Shohreh says they're pushing delegation so we need more audits, cited A350 as an example
Patrick disagreed

Review of WP Section 2.1 – Patricia F./Michel M., definition of intentional unauthorized electronic interaction

Presenting text from ARAC report
Purpose was to clarify, there was no gap

Remove last sentence of 2.1 + change definition of interaction (Action Dan to propose a definition)
This definition should be put in ED-201.

Review of WP Section 3.6 – Patrick Morrissey/Michel M

ED202: Level of threat -> possibility that threat scenario cause a threat condition
Discussion Effectiveness vs. Likelihood

Different definitions of effectiveness in the document
When attacker is most powerful, level of threat increases and in the same way likelihood increases
Is the global effectiveness of the set of security measure enough to block the attack?

Need to be resilient to the type of attacks
Risk= severity*likelihood
Can we consider that effectiveness (even in reverse) is comparable to likelihood?
Dan - in the figure level of threat outside the architecture should be replaced by level of attack
Level of attack = attempts and capability of attempts

Level of threat = the attempts are successful
Bernie - Effectiveness is a component of level of threat, but something is missing
Michel - There is only one evaluation for level of threat and effectiveness

Consensus on: Level of attack minus the effectiveness measured as the intended effectiveness (including discovered vulnerabilities) less the possibility of undiscovered vulnerabilities is equal to the level of threat

Agreement on high level
Challenge for means to evaluate
Patrick goes on and makes a proposal for next meeting

Day 5

Review of WP Section 3.6.1.1 – Chuck Royalty

Based on ED-203 material
3.6.1.1 Figure 3-1 could be replaced by the one in ED-203 Appendix D, or another one to be drawn based on this one.

3.6.1.2 shows the link between architecture, assurance and risk assessment.

Encourage people to provide comments

Review of WP Section 3.4 – David Pierce/Clive Goodchild

Be careful to terminology used and keep it compliant with ED-202
Simplify the figure keeping only asset and security measures considered in the scenario
Discussion about the opportunity to add intermediate threat condition in the figure.

Threat condition is linked to an asset and not to a threat scenario
Bernie proposes to reuse the steps defined in DO-356 much more structured
However it can lead to some redundancies with new 2.3 chapter

Stefan's term – intermediate targets
Threat scenario is a single course of attack, if intermediate target is in there, it needs to be performed in the course of the ultimate target
Dave - Be careful of targets, intermediate targets and functions
Dan - Threat condition is any condition caused by the attack, don't want to rediscover that again, need to change the definition?
Dave - Threat condition only if there's a scenario
Intermediate targets have their own threat scenarios if appropriate which may or may not form part of a larger threat scenario, it depends on the definition of assets and possible attack paths.
Stefan – context, immediate target has its own threat condition, similar to safety, failure conditions at aircraft and LRU level, should have that here as well, pivot attacks, loss of security margin if security breached (Dan agreed)

Chuck – if you can detect, build stronger security measures, architecture with responsive security measures, figure 2-6 threat scenario example is difficult to look at, same box or partition? Indication of security channels between them? Where are you drawing the line?

Dave – later in the document it is more specific, this is an intro to the topic, what might be part of the description

Michel – may not know about architecture for security measure or function, identify threat scenario and later associate with real system items and architecture
Intermediate or not, still need to assess
Correlation between threat conditions and threat scenarios

Dan - Govern security measures as assets as well
Michel - Identify assets and threat conditions either together or separate
Dave – no existing comments except what was received today, will clean up document and post for a final review

Schedule discussion:

Next meeting March in Brussels
A lot of actions and WP reviews need to be complete by March otherwise we will be behind schedule
Need of an agenda for the work to be done since March
Brussels meeting will be at EUROCONTROL which is near the airport, shuttles to and from downtown Brussels (do not rent a car)

Complete draft awaited for June, very ambitious
Probably small working group to be handled
July – last meeting before document released for FRAC
Send copy August 18

Closing remarks

Closing remarks from FAA (Varun) – progress slow but moving, make sure we do not expand scope, organizational and people certification should not apply here (Doesn't want to have independent organization), don't have it for functional side so why should we have for security side, content issues need to be resolved
Ok with process independence

Closing remarks from EASA (Cyrille) - No plan for now to modify Part21 for security, Happy with the atmosphere, constructive

RTCA remarks – until workspace up and running, will continue to post to both RTCA and EUROCAE sites
Thanks to Dan and Honeywell for hosting

Adjourn

/s/
Siobvan Nyikos
Secretary, SC-216
CERTIFIED as a true and accurate summary of the meeting

/s/
David Pierce
Co-Chairman, SC-216

/s/
Daniel Johnson
Co-Chairman, SC-216