AADL standards meeting Sept 25-28, 2017

- Location Fort Worth, Texas, USA
    - Meeting information
        - At the SAE Aerotech meeting,
            - Fort Worth Convention Center
            - 111 W. 4th Street
            - Fort Worth, Texas 76102
        - Register at the committee web page first, it's much less expensive. Then you can register for other events like the tour, banquet, or lunch on the Aerotech site.
            - Pre-registration $189, after Sept 15th $229
            - https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAAS2C
            - You can also register through Customer Service at 1-877-606-7323 ((1-724-776-4970 outside the U.S. and Canada)
        - If you have any questions, please contact Dorothy Lloyd, Aerospace Standards Specialist, at 724-772-8663 or dlloyd@sae.org.

ATTENDEES: Jerome Hugues (JH), Pierre Dissaux (PD), Bruce Lewis (BL), Joe Seibel (JS), Alex Boydston (AB), Frank Singhoff (FS), Brendan Hall (BH), Alexey Khoroshilov (AK), Denis Budzalov (DB), Pierre Dissaux (PD),

ONLINE: Brian Larson (BL), Charlie Payne (CP), Dave Gluch (DG), Philip Alldredge (PA), Dorothy Lloyd (DL), Thierry LeSergent (TL), Chung-Wei Lin, Tyler Smith (TS), Peter Feiler (PF), Dominque Blouin (DB), Gui Goretekin (GG), Tyler Smith (TS), Lutz Wrage (LW)

Monday, Sept 25

- 0900-1000: AADL standardization committee news + action items (Bruce Lewis)

1. BL opened up with news that Peter Feiler is not with us due to helping his wife with a broken arm.
2. BL showed upcoming SAE/AADL Meetings
    2.1. Winter 2018 – Toulouse, ERTS 2018, Jan 29-31, 2018
    2.2. Spring 2018 – Baltimore, May 7-10, AS-2
    2.3. Fall 2018 – London, UK dates - Discussion on the location of the meeting and when and exactly where it would happen.
3. Behavior Annex Awards – John Pierre, Dennis Budzalov, Brian Larson, Etienne Borde, Peter Feiler
4. Ballots to stabilize older Standard Generic Open Architecture from AS-2A – This was a committee that existed before AADL. They inherited this Generic Open Architecture from AS-2A. They have to ballot this. They would send these out for committee. This has to be done every 5 years. Dorothy

said that the AS-2A is inactive. The idea was portability like FACE and having portability. Could we use an SAE AIR for FACE-AADL Annex.

5. Bruce said that he didn't know if an FMI Annex will be needed or not, that is part of the investigation.
6. Jerome mentioned that in addition to FACE-AADL to make sure that SAE ARP 4754, SAE ARP 4761. It would be good to have an AIR for this. The paper that Julien and Peter worked from SEI could be made for availability.
7. Brendan Hall mentioned that Frank Williams of Boeing is talking about a standardized SysML framework.
8. STPA could be added to for an annex. The lessons learned that we are having. There is work with the ARP 4754 and 4761 updates on use of STPA.
9. The ability to capture the interfaces (data and behavior) of FACE Components to facilitate virtual integration and analysis of the components.
10. Dave Gluch asked about the STPA with respect to Security. Mention of Col Bill Young's STPA-Security Dissertation is trying to be obtained but USAF is holding up on the release of it.
11. Behavior Annex, ARINC 653 Annex, Network Annex, Security Annex, Data Annex, Code Generation Annex, Need an updated EMV2 to update with the Behavior Annex
12. Russians: The Error Model Annex could be extended with the Behavior Model Annex
13. Brendan Hall: The EMV and BA doesn't necessarily have to merge.
14. Brian Larson: How dispatching is done on internal ports. On the Error side it has certain types and in the Behavior certain types. It would be great to have some project. Bruce said probably need to explore that further. Need an example to show how to do this. Brian side that they had a coupling annex. Worked on a couple of years but no example exists.
15. ACTION ITEM: Brendan suggested an AIR example for this interwork with EMV and BA.
16. Jerome brought up a lot of points on Behavior modeling.
17. Brendan mentioned some points on a hybrid.
18. Brian Larson: On Department of Homeland Security ISOSCELES is program.
19. Discussion on the need for a GUI for the Behavioral Annex was brought up by Alex Boydston. It was found in the recent demonstration that AADL was weak in Behavioral Analysis.
20. Pierre Dissaulx said that it is important to define what is important to model and analyze.
21. Bruce brought up the planning for Toulouse

- **1000-1100 Security Annex Overview (David Gluch, Sam Proctor, Bob Ellison, Eugene Vasserman)**

22. Objectives and Expected Outcomes – Wants to establish an agreed upon set of capabilities, identify and discuss implementation approaches, clarify and or define and document differences
23. Security Annex Capabilities
    - 23.1. Security Requirements and Policies
    - 23.2. Security Threat Modeling
    - 23.3. Security Requirements and Policies
        - 23.3.1. Do you want to generate the security policies from the model?
        - 23.3.2. There may be specific cases where you have architecture configurations.

23.3.3. Generate the authorizations and configuration policies.

23.3.4. What kind of things that you are going to generate? Is it Active Directory settings?

23.3.5. Modify to architectural aspects and not get down to the specifics.

23.3.6. Whether they use two factor authentication or password only we don't want to make that judgement.

23.3.7. Implementation Considerations

23.3.7.1. Higher level properties are considered goals in ALISA / OSATE

23.3.7.2. All of the security policy requirements would be in the tools.

23.3.7.3. Annex establishes a framework for using AADL and ALISA / OSATE.

23.3.7.4. Assurance cases to ensure that you've met the requirements.

23.3.7.5. Dave Gluch does not have an example to show.

23.3.7.6. We have an error annex but not a safety annex. Later he proposes that they use the EMV2 to do the security work. Want to talk about this.

23.3.7.7. BL said that Peter Feiler thought that EMV could apply to Safety and Security too.

23.3.7.8. Pierre said that the Behavior Annex could be applied because of the nominal behavior of the system. Dave Gluch said that the BA considers nominal behavior but the Error Annex already deals with aspects that security applies.

23.3.7.9. Dave Gluch – If we want to use the Bell-Lapadulla modeling we could use what we have. We need to augment a lot of the capabilities to support a comprehensive capabilities. Bruce Lewis – The annex would capture areas that would be of interest. The ALISA could capture requirements. Dave said that with requirements and modeling the approach could help with the modeling. He said that he could continue to work. Brendan Hall – We know that there is a list of vulnerabilities. Is there a mapping of the CWE (Common Weakness Enumeration) applied? Certain things to not do (e.g., allocating buffers). ACTION ITEM: Brendan Hall said that the properties needed.

23.3.7.10. Alex Boydston mentioned that STIGs need to be considered. Also, RTCA DO-326 and RTCA DO-356 needs consideration.

23.3.7.11. Brendan Hall asked if we are considering primitives such as firewalls.

23.3.7.12. Charlie Payne suggested that he didn't recommend firewalls and VPNs be the representations, but rather the policies.

23.3.7.13. Access Control & Protection – Capability to model assess, and assure security access control including single and multi-factor authentication, authorization, access permissions, access management, non-repudiation, isolation , specialized models (Bell-LaPadula, Biba), Intrusion detection and recovery, protected containment.

23.3.7.14. Dave Gluch talked of using Resolute for capturing properties and libraries, claim and computational functions and prove capabilities. He has been working on Julien's previous work.

23.3.7.15. Cryptography and Containment – Should be able to model and assess that they are there. Do you want to wrestle with key management? Do you want to get into the PKI? The distribution and management of keys.

23.3.7.16. Brian Larson – We only want to represent what is in the system boundary and not the entire things necessary for a system boundary.

23.3.7.17. Charlie Payne – Don't necessarily what produced a CRL, but what is needed in the boundary of the system.

23.3.7.18. Dave Gluch – Main concern is if we need to do this with or without the key management. Anything that is related internally such as got an updated key.

23.3.7.19. Charlie Payne – Agree that key management inside the system boundary is of interest.

23.3.7.20. Dave Gluch – Thinks that AADL has mechanisms to deal with the security without any changes.

23.3.7.21. Jerome Hugues – Authentication and encryption is handled. Curious if they could cover the needs. Not sure what is applicable to AADL with respect to the security policy.

- 11:00-11:30 break
- 11:30-12:00: Security Annex Discussion continued

1. Action / Command Protection
   a. Capability to model, assess, and assure access control of execution of actions/commands including security kernels, OS security controls, etc.
   b. That seems reasonable
2. Security Architectures
   a. MILS, D-MILS
   b. Secure kernels
   c. Dave Gluch is concerned with how to put together the Security Annex because it is so sweeping.
   d. Is there more on Isoceles that can be further discussed? Brian Larson said that he couldn't at this time. It would be good for showing interaction of EMV2 and Behavior Annex.
3. Threat / Attack Modeling
   a. Should we be addressing this?
   b. Thinks that this should be put on hold because it deals with the environment than the system.
   c. Capability to capture & analyze threat/attack models including: Attack/attacker models, attack surface models, attack trees, chain of events models, attack patterns, denial of service.

    d. Capability to identify, model and analyze security vulnerabilities: Architecture/code defects, malicious code, misuse/improper use.
    e. There are a lot of similarities between safety and security. What would cause problems.

4. Summary – Issues and Discussion Topics
    a. What is the difference between isolated partitions and security kernels? Kernals can support partitions.
    b. Questions on what the difference in authentication, encryption, authenticated encryption.
    c. Difference between trustworthy and trust.
    d. Issue of security certification. Common Criteria Capability is what the US supports. There is an agreement between countries for security approach. Within the US DoD there are certain criteria that has to be followed. Each country may have their own, but what AADL is addressing would be more of the Common Criteria.
    e. Merging Safety and Security Analysis – Wasn't an advocate at the outset, but now Dave is realizing that there is commonality across this so that safety and security can work together. RTCA D0-236 and DO-356 are references to consider.
    f. Frank Singhoff – What are the analysis and the properties that are needed.
    g. Dave Gluch said to send him an email if there is more that needs to be provided.

- 1200-12:30: Demonstration of FMI using AADL (Jerome Hugues)
    1. AADL has multiple capabilities for analysis. Model level simulation. Model Checking (FIACRE, Ocarina/LNT)
    2. Code Gen.
    3. 1 year study
    4. Studying the interplay between AADL and FMI standards.
    5. ACTION ITEM: Need to ensure that Amanda Nappier gets the no-cost extension established via contracts.
    6. FMI is an Open Standard on Functional Mockup Interface
    7. Strongly connects physics and control/command.
    8. Implemented by executeable FMUs. FMUscan be connected.
    9. Use FMI for Model Exchange and CoSimulation.
    10. Model Exchange is not as effective/interesting as cosimulation.
    11. Cosimulation requires synchronize the execution blocks.
    12. Allows for solving differential equations.
    13. There will be a technical report at the end of the study.
    14. Master algorithm for co-simulation. Instantiate and initialize each FMU. For each FMU at communication step: values exchange and step calculation. Time based or event based.
    15. They performed a use-case with a basic moonlander.
    16. They modeled in AADL.
    17. They integrated the FMU combining everything. They took the AADL system and converted to process model.
    18. There has to be some timing synchronization of the system.

19. Check the coupled model. Outputs ->Inputs types compatibility. Ports causality and variability (events, data)
20. You may have multiple clocks (say 2).
21. FMI wants to protect the IP.
22. Build or generate the master algorithm. Generate C code. Need to compute the dependency graph.
23. FMU contains the differential equations in a compiled format protecting the algorithms.
24. With this a simulation can be run with OpenModelica and AADL working in conjunction with one another.
25. FMU2AADL Toolkit – Leverages FMUSDK2 from Modelion
26. This is available at https://githumb.com/Samares-Engineering/FMI
27. ROSACE: https://svn.onera/fr/schedmcore/brances/ROASACE_CaseStudy
    a. Can test 3 FMUs at once
    b. Brendan said that SCADE has FMU support.
    c. Claire Pagetti, David Saussie, Roman Gratia
28. Crazyfile – Affordable, tine and versatile UAV, https://www.bitcraze.io
29. Part of the GaTech Class.
30. ANSYS is doing student competitions
31. There was problem with the Simulink export.
32. AADL Inspector is currently not working with FMI.
33. Brendan said that once you start interoperating with AADL and FMI then interesting co-simulation work can be done.
34. This would allow testing at the systems level in the model.
35. Brendan mentioned VISTIS for virtual integration.
36. AADL covers mostly discrete time. FMU interconnects also continuous.
37. Simulation model derives from Systems engineering model. AADL and FMU refines subsystems. See OpenCPS project.
38. How to map errors from FMU to AADL error events. Mostly convention, mutable states vs. internal ports.
39. Brendan was talking about integrating SysML with this.
40. Brendan brought up MCDC for architecture with use of FMI and AADL. Jerome said oh no no no.
41. Showed FMI/SysML Efforts
    a. http://www.sysml4industry.org/?page_id=242
    b. https://into-cps.github.io
    c. https://www.opencps.eu

- **1230-1400: Lunch**

- **1430-1630: Network Annex Draft Review and Update (Alexey Khoroshilov, Brendan Hall)**

1. Graphical User Interface (GUI) for BLESS will continue to suffer without it.

2. Brian will send a suggestive write-up for topic for GUI for BLESS. They want simulation in addition to graphical representation.
3. Philip asked if he had any ideas of the GUI he wanted. Wondered if the Sequence Diagram from SysML. Brian said that PVISO would be a starting point, making it look like what SysML is using. At one time he thought of all of the states being on the periphery. Very open to what it looks like. Philip said that the API would have to be tailored. Brian said that the RFP proposal would need to be submitted.
4. Alexey – AADL Networking Annex Status Report
5. Content of the Annex. Got feedback from Steve Vestal and Brendan Hall
6. Most recent version is located at https://gitlab.com/sae_as2c/networking-annex/wikis/home
7. Feedback from Steve Vestal
    a. Properties for End System ID and Switch ID (0..65535)
        i. Need to have identification of devices in the model.
        ii. Use similar model but called an identifier.
        iii. Alexey thinks that this shouldn't be in the annex because it is too specific.
        iv. Jerome Hugues said that this would be specific for configuration management.
    b. Max_Supported_VLs
        i. Thinks that it is appropriate to have such a property.
        ii. But the property is useful for these models.
        iii. Dennis Budzalov asked why is the inheritance is necessary.
    c. Not necessarily require switches and end systems be modeled using a single specific category or pattern.
    d. End systems in particular may be combinations of multiple software and hardware components. ACTION ITEM: Need to speak with Peter Feiler.
    e. There will probably need to be some sort of patterns or modeling conventions defined in order to make tool development reasonably feasible (the ARINC 653 annex does this some, e.g., the pattern for a partition is a process hosted on a virtual processor). Alexey said that he wasn't sure about the inheritance need with AADL v2.2. He said that inheritance could be used for now and switch to library in AADL v3.0.
    f. Brendan Hall recommended that an AADL model of network is needed in the future. Suggested use of JMR MSAD to be a user of the Annex.
    g. This networking annex is initially geared to ARINC 664.
    h. Brendan asked what the relationship is between ARINC 653 and ARINC 664. (ARINC 653 is partitioning and ARINC 664 is a rate constrained network. Per Alexey, there can be a relationship with the I/O. They are not tightly bound. Depends on being a driver.)
    i. Steve mentioned "Routings can be tree structures [multicasting], the standard AADL connection binding properties are not adequate (they only allow single linear sequences of objects as a routing). The least bad interim approach would be to

define a **custom connection binding property** that is a linear bindings, with the legality rule that the set of linear bindings must show a pattern of common prefixes that allows them to collectively be interpreted as a tree.

j. Brendan said that Network Configuration files can be rather large…Do you want to embed that in AADL?
k. Dennis Budzalov – Different virtual links use the flows. Size of the external files can be reduced by reusing the model elements. The idea of trees is nice, but the implementation is setting is ????
l. Brendan Hall suggested a configured database to do some analysis for some target system.
m. Dennis asked where is the line of what should be in the database versus in the model. We look at the model itself as a database. Try to treat the model without touching with hands. To understand this opinion, not thinking about separate files or database.
n. Brendan – Use of the AADL file could create an ecosystem.
o. Alexey – Use the external file to keep up the configuration; however, you have to create semantics to keep up with the information.
p. Brendan – Do you then not need a format to do that.
q. Alexey – In his experience it is tool specific. We can exchange forms in AADL. Importation with well-defined semantics. Trying to make the model so….
r. There is a lot of challenging tools to keep up with this.
s. Discussion of multicast with respect to the Networking Annex came up.
t. Rate Constraints came up with respect to the segments since this is ARINC 664.
u. There was a discussion about using common prefixes and suffixes between Jerome and Dennis.
v. Virtual links with end-to-end flows were discussed between Jerome and Dennis.
w. Want to have model elements with certain properties for configuration elements that would be applied. Could apply properties to end-to-end flows.
x. Dennis: The idea is to use flows in virtual links.
y. Jerome: Are you binding a virtual flow to a processor system?
z. Dennis: IDs….Historically have no hardware falls. It’s mostly about subnets.
aa. Jerome: It’s a lot to bind a virtual busses to a processor.
bb. Dennis: Only binding a virtual link in software.
cc. Alexey: CPU have implementation…
dd. Alexey: Postpone this discussion with Peter. Agree to limit scope to get something out.
ee. Jerome: Steve have concept of flows

8. Old Action Items
    a. AI2: Add ref model a model of end-to-end protocol on top of AFDX virtual links.
    b. AI3: Describe safety properties of AFDEX components from the ref model with EMV2.
    c. AI4: propose recommendations how to model ICD in AADL.

    d. AI5: Update TTEthernet ref model and organize it review by TTTech.
    e. Brendan suggested that perhaps some of the AFDX Network Annex.
9. Alexey: Suggested that binding of multicast with processors needs to be generated.
10. Brendan: Want to demonstrate the AADL Cross Domain Analysis. Take the 4761 Wheel Braking System to mitigate issues. Maybe something we add in an AIR. Someone would have to write that up.
11. Alexey is not right now generating the ICD but is moving in that direction.
12. Alexey stepped through the draft of the Networking Annex which showed the properties and semantics of the annex in AADL.
13. There was some issues in showing the document. Bruce noted that the format would have to be improved before submission to SAE.
14. Bruce asked if they want to provide a sample document to see if they can process it.
15. Alexey said that by end of this year should be able to provide a document in format that would work.
16. Bruce asked if we are reasonably close to balloting this.
17. Alexey said that they would want to get the document would want to clean up the document and get reviewed. Before the ballot the draft with two open items to be discussed with Steve Vestal and Peter Feiler.
18. Bruce said that we are pretty close.

1730-1800: AADL Workspace Definition (Pierre Dissaux)

1. Ellidiss Technologies – AADL Workspace
2. 10 years of work in AADL Tools.
3. AADL language itself is good.
4. Small issues – boundaries of current project, how is common environment defined? What remains specific to a particular tool?
5. Tools: Stood, TASTE, Inspector, RAMSES, Capella, EEA
6. What is tool specific and what is language specific?
7. Property sets should be shared with everyone.
8. At tool level customized with the language.
9. Restrict scope of the language with subset.
10. The use of Feature Groups is complicated. Should be in the global AADL property set.
11. Make the name of the root instance in AADL itself.
12. AADL Workspace recommendations
    a. Better define the various levels of configuration in the next standard
        i. Official standard
            1. Core syntax and semantics
            2. Predefined Property Sets
            3. Standardized Annexes
        ii. Tool or usage profile (tool configuration)

        1. Non-predefined Property Sets
        2. Non standardized annexes
        3. Subsets
    iii. Project or model (user workspace)
        1. List of Packages

Tuesday, Sept 26

- 0900-1030: AADL v3 discussions (Compositional Interfaces) (Peter Feiler)
- 1030-1100: break
- 1100-1130: Continued (Compositional Interfaces)
- 1130-1230: AADL v3 discussions (array connections, unified type systems)
- 1230-1330: **Short** Lunch
- 1330-1500: Attend Aerotech Session ATC405
  - 1330 Using multicore processors for safety critical avionics (Wind River)
  - 1400 Better Reuse of Architecture Models: Profits and Costs (Denis Buzdalov)
  - 1430 Adopting Model-Based Software Design and Verification for Aerospace Systems (UTC)
- 1500-1530: Break
- 1530-1600: Continued (array connections, unified type systems)
- 1600-1730: AADL v3 discussions (Configuration & Binding) (Peter Feiler, Alexey Khoroshilov, Denis Buzdalov)

- **AADL v3 roadmap review (Peter Feiler)**

1. Peter Feiler
2. Put out version 2.2.2 of OSATE
3. New draft document for SAE. Jerome will be in Pittsburgh in early December to work document content.
4. Prototyping for version 3. Lutz started working this prototyping and the language grammar for the programmer. Working on the metamodel so that it can be woven into the current version of AADL. The meta-model hasn't changed much from V1 to V2.
5. Will be prototyping since the interface will be coming up and the binding part is coming up.
6. OSATE Infrastructure Cleanup – Joe Seibel and Philip Addridge been working. Less dependence on Eclipse is being sought for.
7. Compositional Interface – This has been worked on quite well. Should be able to provide draft parts of the text on this.

8. Configuration and Choice Points are being worked on.
9. Binding concepts – This is currently being done through properties. This will make it an explicit concept. This will address some of the AIPD TIA partner complaints to binding to processers.
10. The Constraint Annex has been put on hold. Serban retired. Can come back to this after version 3. The Constraint Annex had overlap with other annexes such as Behavioral.
11. Array support revisited. Exposure of index dimensions/sizes in interface via feature arrays. Connection declarations with embedded index specification. Configuration of dimension sizes.
12. Roadmap Candidates
    - a. Multicore – Jerome will be talking about standards
    - b. Virtual platforms – includes virtual memory. Comes in handy with security modeling. Support of hardware flows through platform. Virtual platform flow gets bound to hardware down below. There initially was only 3 types of binding. The new binding mechanism will improve binding.
    - c. ACTION ITEM: Brendan will look at some configuration examples of virtual integration of software to the hardware platform. Work at a high level and put on a target implementation.
    - d. Peter said that we couldn’t do that well before because it was hidden as a property itself.
    - e. Unification systems
        - i. Data types, property types, constraint language types were different. They have been working on a single underlying type.
        - ii. Standard unification of the system.
        - iii. See slide 10.
        - iv. Property set names.
    - f. Flow Trees and graphs – Came out of JMR AIPD – Working on improving.
    - g. Improve specification of ports for data or event ports. Do we want to expression?
    - h. Dennis Budzalov: For ports don’t you want what was originally a category of ports to something that was optional.
    - i. Brendan: Do you want to consider the ports for the physical flows or are we going to discrete flows? More for the Error Model. We need to talk to the continuous pipe.
    - j. Dennis: The 2.2 ports have problems with freezing. We have problems with ARINC 653 ports with AADL ports. We probably need to leave in standard but making more flexible.
    - k. Jerome: We do need to revisit them with respect to the dispatch environment. Need to consider the ARINC 653 to be discussed.
    - l. Dennis: The freezable ports for buffering can be useful, but a range of ports needs to be considered.
    - m. Peter: We can move around some of the smaller items and pick up some features at the next meeting.

n. Bruce: Brendan mentioned doing something for functional as opposed to abstract.

o. Brendan: Would it be good to have a functional item? A lot of people are pushing functional, logical and physical. Does that make sense? This was experienced on SAVI. Are we going to say function is abstract.

p. Peter: One thing that is confusing is that the abstract has 2 roles. (1) Generic component like SysML, (2) have something that you specify later as a particular implementation. Abstract feature and generic component – Need to simplifying. Keyword is FEATURE and on a component is an ABSTRACT.

q. Physical FEATURE vs Physical PORT – Peter recommends Physical FEATURE.

r. Dennis Budzalov – busses represents wires. It is not really clear, talking about hardware features of busses.

s. Brendan – We've overloaded terms. We keep as discrete signal flow in one form or another. A whole discussion about safety terms and use of terms that are overloaded. Bruce said that this is something that Peter has been thinking about but we can't take too much time on it.

t. Peter – This is an example on a topic that we can keep up and figure out for version 3.

u. Brendan – Proxy to do error annotation.

v. Peter – One thing is to think about other modeling annotations and is there something good to use in AADL. The notion of a continuous connection point version a discrete connection point.

w. Brendan – The Wheel Brake System example is an example of using this.

x. Dennis – We usually use a chain of …we have a process….a set of logical connection in a platform and we have a processor that has bindings. In this way we don't have confidence that we have ability to putting faults in lower levels.

- **AADL v3 discussions (Nested processors, virtual memory & memory configurations) (Peter Feiler, Alexey Khoroshilov, Jerome Hugues)**

1. Configuration of a System Design

   a. Peter discussed configuring subcomponents using the "extends" command.

   b. Any subcomponent is a choice point

   c. Finalize subcomponent classifier to a specific implementation.

   d. Example was shown (see slide 4).

      i. Configuration Top.config_L1 extens top.basic

```
{
        Sub1 => x.i,
        Sub2 => y.i
}

System implementation top.basic
```

Subcomponents
Sub1: system x;
Sub2: system y;

Should configuration include a category keyword: (e.g., system configuration or process configuration? Dennis said no.

Comma as separator or semicolon as terminator? Either works.

2. Peter went through Previously Configured Subcomponents
    a. Brendan: Are you allowing connections to be defined in a configuration blocks?
    b. Peter: Once I get to the basics I will provide examples.
    c. Brendan: Not sure if it is a good idea. Just want to know what you thought about this.
    d. Peter: Not sure if I have this on the slide.
3. Configuration Assignment Rules
    a. Similar to refinement rules
        i. Type to implementation
        ii. Implementation to implementation extension and configuration
        iii. Replace with configuration only
        iv. Replace (default) implementation (current classifier match)
        v. Type extension
    b. Configuration can be used as classifier
        i. Implementations cannot extend configurations
    c. Dennis Budzalov had some comments about this approach. Said that Peter was trying to think for the user. He said that this rule could lead to bad modeling.
    d. Peter asked if we want to allow an override of an implementation with another.
    e. Whatever rule that is decided on will be checked for in the AADL compiler.
4. Configuration of Property Values was presented.
    a. Be able to specify elements to be used in a configuration
    b. A configuration specifxcation with only property associations acts like a data set that applies to a design. It can be combined with others through configuration composition.
    c. Equivalent to myps::security_level => L2 applies to Sub1.
5. Property Values as Parameters were presented.
6. Parameterized Configuration was shown to fill patterns of holes left.
7. Peter showed Explicit Specification of Candidates.
8. Dennis Budzalov told Peter that he was working with Union Types. Said that this contradicts with Brian Larson's philosophy. In discussion with Steve Vestals comments on the Network Annex we ran into Union Types for properties.
9. Do we need Unions or Sections on the categories?
10. Dennis Budzalov thinks that we definitely need to this.

11. Peter Feiler said that this has implications on the subcomponents as well.
12. Nested Configuration was skipped over
13. Composition of Configurations Revisited. Adding in flows where flows may be declared in a separate classifier extension. Dennis Budzalov – We can configure an AFDX switch. It would look like a pure configuration. What he is suggesting is an implementation. Flow types is what is being suggested and not Flow Specifications. Peter said that configuration is choosing classifiers and the notion of composition of elements of a base configurations.
14. Peter showed Parameterized Configuration example with Safety and Security.
15. With the JMR work do we have the ability to work with flows.
16. Configuration of Annex Subclauses – Peter showed an example of "System" for Different annex specifications. He said alternatively could use "subclause"
17. Peter covered Name Path Based Composition. There was a keyword of "unsafe" and "unchecked" was suggested instead. Then later "deferred" was a better word.
18. Arrays and multiplicities were discussed.
19. Brendan suggested that these slides be sent out. Peter said that he would send this out.
20. Dennis asked if this was recorded and Bruce said that this wasn't.
21. Need for Prototype and Refined To? Suggested that the Prototype mechanism can be removed. No one had any comments on either of these.
22. Bruce asked what about the conversion of version 2.2.2 to version 3.0?

Wednesday, Sept 27

AeroTech – 8:00-9:00 Kristen Baldwin on Cyber Security

ONLINE: Dominque Blouin, Gui Goretekin, Tyler Smith, Lutz Wrage

- 0900-09:30: AADL Runtime Services (RTS) Mid Meeting Recommendations (Jerome Hugues)
- 0930-1000: AADL Runtime Discussion (Jerome Hugues, Brian Larson, Etienne Borde)

1. Initial objective to discuss formalization of the RTS
2. A.9 (31) section – RTS is defined as AADL subprograms with in parameters and SendException:out event data. Send_Output runtime service allows the source text of a thread to explicitly cause event, event data, or data to be transmitted through outgoing ports to receiver ports.

3. A.9.2.4 (31) The output is transferred to other components at completion time. Property in declarative model? EMV2?
4. With RTS how do I implement AADL subprogram/thread (This is the primary objective). Do we want a "portable" RTS that would allow separation between code generator and AADL runtime.
5. Some elements struggled with…
    a. How are the dispatch conditions (e.g., BLESS vs BA) handled? Are they hanled inside the services or are they handled in application specific infrastructure code? Defininiton of Dispatch_Status?
    b. Need to address the complexity of the dispatch conditions. How to perform runtime monitoring? Security or Safety?
    c. What kind of error events we want to propagate? How do we handle?
    d. Recovery points….How do we deal with.
    e. There are problems with notions of Freezing Variables…Should this happen in the dispatch mechanism or through receive_input? This deals with safety mostly.
    f. Want to avoid deadlocks and stupid use by stupid users.
    g. Get_Count – need to understand the interpretation…What does <<new>> mean, which time reference? New in the list of frozen port, since previous freeqing? New value that we received since current freezing period, not yet frozen and thus not visible? Wahat if we call it multiple times? If we do a Get_Value ? Is the value constant?
    h. Dispatch conditions allowed? Dequeue protocols? Dequeue item? Port Queue Processing?
        i. Queue size, Overflow_Handling_Protocol, Queue Processing Protocol, Urgency (timing).
6. Roadmap
    a. Will be part of AADLv3 discussion
    b. Select model of computations /scheduler we want to support
    c. Review properties that are desirable or dangerous
    d. => modeling subset with attached semantics and then revisit RTS definition and semantics
    e. Should clarify the AADL core. Need a formal proof or conformance test of runtime.
7. Need to review the dispatch protocols.
8. Bruce asked what Jerome meant by a formal proof.
9. Jerome said that given a set of elements in architecture there will not be any errors and system will not crash. You would make sure that the composition would be correct by construction.
10. Bruce said "So, when you do 'correct by construction', you are checking for no runtime errors, right". Jerome, "yes".
11. Brian Larson said that "Correct by construction has been the whole point of BLESS. BLESS has simple definitions. It is not good for all cases. It will be interested if we can do code generation and being able to do dispatching and freezing. This is simple enough to have

formal definitions to have compositional correctness of a configuration or assumptions with what will happened with receipt of information on a port." "Assumptions about dispatch conditions with timeouts is considered." "There are a few other things added that is not in the standard (e.g., timestamps)".

12. Bruce asked what would be suggested for next meeting. Jerome said he would have to wait until visit in Pittsburgh. Jerome said this could be done in 2 hours.

- 1000-1030: break
- 1100-1130: Behavior Annex Errata (Pierre Dissaux, Etienne Borde)

1. Behavior Annex v2 AS 5506/3 released August 2017
2. Open Issues shown on wiki (hppts://wiki.sei.cmu.edu/sae-aadl-subcommittee/index.php/Errata_from_the_Behavior_Annex
    a. Expressions as parameters of computation instruction
    b. Exceptions
    c. Local and loop variables
    d. Status of Behavior_Properties property set
    e. BA formal semantics
    f. Better formalize the core run-time semantics first
3. Discussion about addressing some problems in the core language between Dennis Budzalov, Pierre Dassault, and Brian Larson occurred.
4. Action Item: Bruce to add a discussion on Exception Handling Classification to the agenda for Toulouse, FR meeting for set of alternatives to consider. Dennis can present some thoughts on addressing how which decisions in the core language can affect the BA but will not present a solution. Dennis said that he could attempt to present a short presentation to see if this type of work is productive or not. (Bruce: This will be dependent on the runtime services.)
5. Pierre Dassualx said that they are using the Behavior Annex in Cheddar.
6. Dennis Budzalov said that in MASIW that they use it some. He did some presentations some time ago. They have specifications for hardware competence. They support 3 types of specification.

- 1130-1200: AADL Core and EMV2 Errata (Peter Feiler)
- 1200-1230: AADL Core and EMV2 Errata continued

1. Peter said that he has some Errata on EMV2 to touch on. Tyler has some things on EMV3.
2. In terms of OSATEv2.2.2, Steve Vestal pointed out that when you do end to end flows you can specify the component or subcomponent. Some editorial issues that need to get corrected.
3. Some things were reported out as an error will be corrected to not report as an error.
4. These will be an editorial correction. Peter will follow up with Joe Seibel
5. Switching over to version 3 Tyler suggested some things such as "not explicitly declaring 'thread'"
6. Joe suggested that an abstract classifier but a concrete subcomponent.
7. Bruce said that he wants to make things readable.

8. Joe said that the keyword could be optionally used.
9. It was noted that the "with" is not a true import.
10. Thread groups – Can we have interface implementations without enforcement. The general philosophy of AADL is to have conformance.
11. Tyler said that if I am wanting to write the model quickly and I want to have features.
12. Peter said that you might not want to write a separate declaration….????
13. Joe Seibel said that if we want a simple example with a couple of threads.
14. Joe said "Perhaps a separate subcomponent features or a subcomponent subcomponent." Both Tyler and Dennis agreed this would be useful. Dennis said that it would be good to not have to multiply specify.
15. Pierre didn't agree. He said that you needed separate specifiers.
16. Broke out
17. Error Type Library: it goes into the package. Allows you to have multiple elements in a library. Need to be able to represent them in some way. You can still use types. Need to figure out if this could come out in an errata.
18. Error Propagation Declaration – Declaring error propagation by defining a featurereference. Also, you can define an error containment. Dennis Budzalov liked the suggested commands. Brendan said that he would keep "in or out" port.

-

- 1230-1400: Lunch

- 1430-1500: Update on Cheddar - reviewing Multi-Core and ARINC653 plus new features for architecture exploration and integrated Security, Safety, and Scheduling Analysis. (Frank Singhoff)
    1. Multiprocessor scheduling analysis with AADL Inspector/Cheddar
    2. Typical multiprocessor scheduling analysis: partitioned vs global
        a. Decide which processor or core to do this.
        b. Global scheduling – 15-20 years ago you would manage resources and call on processor to pick up the tasks..
    3. Both approaches have been implemented in Cheddar. Global scheduling has really stayed in research. For what you have in AADL inspector you have partitioned scheduling. You can run scheduling analysis.
    4. Fort the PAESA (Pareto Archived ….) There is no relationship with ARINC 653
    5. Shared resources between processing units – Cache units, bus, NoC….You need different scheduling metholds
    6. CRPD – Cache related preemption delay. To be able to deal with this you have to bound the data. There is no efficient way to bound CRPD today.
    7. Cache/CRPD-Aare Priority Assignment Algorithms – Trying to put cache models in aADL.

8. Cache aware scheduling simulation. When you do a simulation and have cache in the loop it gets tricky.
9. Today there are very few tools for scheduling simulation.
10. CRPD is difficult to credit. You have to bound it.
11. The CRPD that you model is oftentimes different than what you are on the system.
12. You can get a proof that your scheduling is good; however it is not easy.
13. This is doable with L1 Cache, but difficult with L2 and L3.
14. Bus could have contention. From a theoretical point of view, yes, but from practical view, no.
15. Network of chips the systems are complex. This is a type of grid.
16. In summary – 1. Multiprocessor scheduling analysis features. 2. Software design space exploration : partitioning with competing objective functions.
17. Trying to develop partitioning with competing objective functions.
18. Tradeoffs with several competing criteria / objective functions such as performances vs safety vs. security.
19. They did a small example with a system running AADL sub-programs.
20. Competing objective function in software design space exploration.
21. Look at several tradeoffs
22. PAES : a multi objective metaheuristic – See slide 13/16. Steps
    a. 1) Mutate a solution to generate a new candidate: small change to move from a solution to a nearby neighbor
    b. 2) Evaluate the mutated solution (conflicting objective functions)
    c. 3) Update non-dominated solutions set (i.e., archive)
    d. 4) Select new solution for next iteration: mutated or current solution.
23. Competing Performance Criteria in the Software Design Space Exploration
    a. Tradeoffs include Min (Preemptions, Max (laxities), Min (ravenscar data blocking time)
24. Conclusion
    a. Multiprocssor scheduling analysis of AADL Inspector & Cheddar
        i. Bund of classical partitioned vs global scheduling algorism
        ii. Shared hardware resources: cache, NoC
    b. Multi-objective partitioning
        i. PAES based, for Ravenscar compliant architecture
        ii. Safety & performance & security objective functions
        iii. Follow Security Annex
25. With cache management the scheduling is very limited to date.

- 1400-1430: Discussion on Multi-Core SHIM initiative and fit with AADL (Jerome Hugues)

1. CFG – Control Flow Graph would have to be modeled for AADL
2. Could be very specific to particular analysis.
3. Standards for dealing with MCP. If we have to integrate amount multiple standards.
4. There is a part of the feature that is mission.
5. The question is if there is a modeling SHIM
6. SHIM - SOFTWARE-HARDWARE INTERFACE FOR MULTI-MANY-CORE

- 1500-1530: Break

- 1530-1600: SCADE AADL Update, ICD for ARINC 664 (Guliherme Gorethkin)
    1. Over the past year or so been creating an AADL authoring tool.
    2. Overview of SCADE Suite and SCADE Architect
    3. SCADE Architect – SysML based. They have all but the Requirements Diagram
    4. SCADE AADL Solution – They don't plan on doing the analysis part, just the authoring part.
    5. Mapped from AADL over to SysML
    6. The annexes are through a different mechanisms.
    7. They chose only parts for AADL to implement.
    8. They have inlined the AADL Abstraction and Inheritance
    9. They took the Prototypes & Abstractions, Components Types, and Components Implementation to AADL components. They have taken the components Instance to Replication.
    10. Roundtrippping would not work at this time.
    11. Jerome is concerned with the things that SCADE is not supporting AADL.
    12. They've made decision to cut back with the SCADE version of AADL to make more simple. They don't support "Extends". This inlines and flattens the whole concept.
    13. Action Item: Look into sending models from AIPD to SCADE to see if the export to SCADE and AADL works well.
    14. They plan to associate the shapes and the symbols from OSTAE.
    15. They have automatic convers from property sets to the adaptations.
    16. He showed a Flight Control example in AADL.
    17. You can take an AADL process and synchronize to SCADE Suite and build in the implementation.
    18. Brendan asked if you could take multiple processors running at different rates.
    19. Could you have multiple nodes and threads to get the emergent properties to the behavior. Brendan thought you could do FMI modeling.
    20. Gui said that they can take SCADE Suite and generate wrapper code around it. Can take the information in the SCADE Architect Model and have the periodicity. He said that this could be possible. Brendan said that he may have something that could be demonstrated.
    21. You can Import / Export into SCADE Architect, Synronized into SCADE Suite and then have SCADE Suite generated code.

22. Bruce mentioned that OCARINA in the SCADE. Jerome said that this was a long time ago and may not work anymore.
23. Gui showed the synchronization of terms from SCADE Suite to AADL.
24. They are acting as the GUI and connection to the behavior part of SCADE Suite.
25. SCADE Ecosystem – Verification.
26. Traceability through SCADE ALM Gateway.
27. Gui showed the actual tool which has a nice user interface.
28. Gui went over the ARINC 664 / AFDX configuration modeling tool with Brake Control System.
29. Brendan said that this can and has been used before for the Network Annex work.

- 1600-1630: Ellidiss STOOD 5.5 and AADL Inspector 1.6 Update (Pierre Dissaux)

1. Methods and Tools for Critical Software Development
2. Behavior Annex and State Machine
3. HOOD – Hierarchitectual Object Oriented Design
4. Stood – Not an acronym
5. They have been following the AADL Annex
6. They have been working multiple projects
7. Space Robotics
8. COTS Tools for AADL – STOOD is not an AADL tool. Generate AADL from STOOD.
9. They have a generator to AADL and an importer from AADL.
10. They mostly work on timing analysis with CHEDDAR with University of BREST.
11. CHEDDAR is what Frank Singhoff presented.
12. AADL Inspector is now Model Inspector because they can now import SysML and MARTE.
13. Model Processing Toolbox : LMP – Logic Model Processor
14. He showed a GUI for the STOOD for AADL Key Features.
15. HOOD is been designed for European Space Agency to promote good engineering processing.
16. Allows top-down modeling processing for AADL.
17. Discussion between Dennis Budzalov and Frank SInghoff about singletons and representation of the textual AADL occurred.
18. The STOOD has a Graphical Editor for AADL, Data hiding, AADL Declarative Model.
19. Modular Analysis Framework was shown which showed several different tools being translated to perform analyses. (Need to get slides).
20. Timing analysis. Safety and Security and analysis to come. Need a demonstration.
21. Pierre went through a tour of the (AADL) Model Inspector.
22. Need a project definition to express the property set.
23. Pierre showed a timing simulation analysis in the tour demo.

- 1630-1700: Georgia Tech Cyber-Physical Systems Class with AADL and Crazyflie (Chris Cargal, Jerome Hugues)
- 1700-1730: Architecture Implementation Process Demonstrations Overview (Alex Boydston)

1. Presented the AIPD Overview
2.

- 1730-1800: Planning for next meeting (Bruce Lewis)

Thursday, Sept 28

- 0800-12:00 – Attend Aerotech. Suggested sessions:

10:30 a.m.	**ORAL ONLY**	**An overview of the FACE standard as applied to a COTS Operating System** *Alex Wilson, Wind River*
11:00 a.m.	**2017-01-2104**	**Multicore Management - A New Approach** *Marc Gatti, Thales Avionics*
11:30 a.m.	**17ATC-0291**	**In flight real-time adaptation** *Bertrand Granado, Université Pierre & Marie Curie; Marc Gatti, Thales Avionics; Julien Denoulet PhD, Université Pierre et Marie Curie; Martin Rayrole, Thales Avionics*

-

Webex Info for the meeting:

```
Monday & Tuesday:

AS-2C AADL
Every day, from Monday, September 25, 2017, to Tuesday, September 26, 2017
8:00 am | Central Daylight Time (Chicago, GMT-05:00) | 10 hrs

JOIN WEBEX MEETING
https://sae.webex.com/sae/j.php?MTID=mc8fe61e7d7a5f5de763b032eb162abb7
Meeting number: 627 949 577
Meeting password: AS2caadl

JOIN BY PHONE
1-866-469-3239 Call-in toll-free number (US/Canada)
```

1-650-429-3300 Call-in toll number (US/Canada)
Access code: 627 949 577

Wednesday:

AS-2C AADL
Wednesday, September 27, 2017
8:00 am | Central Daylight Time (Chicago, GMT-05:00) | 10 hrs

JOIN WEBEX MEETING
https://sae.webex.com/sae/j.php?MTID=m3a5d8b3fbe660daa12f539b285a37b4d
Meeting number: 628 699 262
Meeting password: AS2caadl

JOIN BY PHONE
1-866-469-3239 Call-in toll-free number (US/Canada)
1-650-429-3300 Call-in toll number (US/Canada)
Access code: 628 699 262

Thursday:

AS-2C AADL
Thursday, September 28, 2017
8:00 am | Central Daylight Time (Chicago, GMT-05:00) | 4 hrs

JOIN WEBEX MEETING
https://sae.webex.com/sae/j.php?MTID=m13a2ad9bf7ca58c18fbd347ded8ec3c7
Meeting number: 624 249 560
Meeting password: AS2caadl

JOIN BY PHONE
1-866-469-3239 Call-in toll-free number (US/Canada)
1-650-429-3300 Call-in toll number (US/Canada)
Access code: 624 249 560

Global call-in numbers:
https://sae.webex.com/sae/globalcallin.php?serviceType=MC&ED=591849842&tollFree=1

Toll-free dialing restrictions:
https://www.webex.com/pdf/tollfree_restrictions.pdf