AADL standards meeting Oct 3-5, 2016

At the SEI

Bruce Lewis, Brian Larson, Jason Larkin, Michael Kang, Brian Hulbert, Denis Buzdalov, Alexey Khoroshilov, Jerome Hugues, Frank Singhoff, Julien Delange, Sam Procter, Paul Wortman, Benard Dion, Guilherme Goretkin, Peter Feiler, Lutz Wrage, Eric Feron

Remote:

Brendan Hall, Pierre Dissaux, Immanuel Gidado, Ken Stachelbeck, Jim Carciofini, Steve Vestal, John Franklin, Pierre Labreche ,Roger Champagne, Philip Alldredge,

* Location Pittsburg, PA, USA.
	+ Meeting information
		- At the Software Engineering Institute in Pittsburgh
		- In conjunction with the Embedded Systems Week
		- Sunday morning, Oct 2, tutorial by Julien on Safety and Security, $50 to ESweek
		- Joint workshop with AdaEurope HILT Oct 6,7
	+ No AADL Conference or Meeting fee – tutorials do not require general conference fee, only the fees for workshops/tutorials

# Monday, Oct 3

* 0900-1000: AADL standardization committee news + action items (Bruce Lewis)
	+ Starting on certification of the Ocarina for ESA, Code generation annex would change after that, Data Annex ready to go.
	+ Formal Behavior Annex will be BLESS, combines JP, will have plug-in translation by winter, Will provide document. Will include assertions.
	+ Hybrid Annex – interaction between FMI and Hybrid Annex, **Action-Bruce schedule** time for in next meeting. (HA is continuous behavior). FMI and HA, Cyberphysical systems discussion. Why we introduced Channels. FMI by Jerome, HA Brian and Pavi, Cyberphysical Peter.
	+ Assurance cases – in part in the Requirements Annex. **Action: Peter** could demonstrate at the next meeting. Need to consider how to bring in Assurance cases. Could become an annex. Peter would make a recommendation.
	+ Jan meeting. Jan 30 for the Winter meeting.

* 1000-1030: AADL v3 roadmap review (Peter Feiler)
	+ There will be a new format for the standard. Peter and Jerome working
	+ Will not use Word if we can come up with a new approach
	+ MetaModel Changes – should we simplify it. Pushing the constraints to an external check instead of in the MetaModel. What is the right notation if so. Should we clean it up to make it smaller.
	+ OSATE Infrastructure Cleanup.
	+ Roadmap for version 3.
		- Compositional interfaces now stable,
		- Choice Points and configuration (Peter and Brian),
		- Binding type, binding point, binding instances, ….
		- Is binding the right word, consider what INCOSE uses
		- Platform – nested processors, virtual memory, platforms
		- Property language – Unification of type systems and expression languages (an underlying type system). Includes handling units.
		- (question of compatability – can you convert a current specification to the new?)
		- Property sublanguage –
		- Usefulness of public/private packages (Bren, Jerome)
		- ADL\_Project and project structure (Jerome, Pierre)
		- More Candidates
			* Interrupt handler (Jerome)
			* Data aggregation via protocol
			* Data mapping via new binding/mapping concept
			* Clean up directionality of access features
			* Categories on connections
			* Refinement of categories and features for Abstract components: can we eliminate this? (Adventium is experimenting with, Brian involved, can provide feedback).
			* (error annex maps constraints between errors an modes, internal features allow connection to mode change)
			* Table of contents –
				+ Generic architecture concepts

Components, features, connections/flows

Modes, configurations, instances

* + - * + Specific component categories
				+ Pre-declared
			* Issue- properties should be defined for Threads with the thread concept. We can not define them in another chapter and really understand how they apply (PD)
			* Issue of taking the semantic constraints out of the metamodel. More discussion needed.
* 1030-1100: break
* 1100-1230: AADL v3 discussions (Nested processors, virtual memory & memory configurations) (Peter Feiler, Alexey Khoroshilov, Jerome Hugues)
* 1230-1400: Lunch
* 1400-1430: Continued (Nested processors, virtual memory & memory configurations)
	+ 3 proposals, Virtual Processor no longer contained in a processor, will be done with binding
	+ Nesting is done with the system concept
	+ Virtual buses taking the same approach.
	+ Jerome – how will we represent the switch,
	+ Using abstract components and abstract features, do we distinguish between non directional and bi-directional. New SAVI model is using abstract instead of buses.
	+ Physical features – continuous flow vs discrete. How many do we need? MILS/AADL has physical and observation point. Observations could be discrete or continuous. Observable could be model checking reasoning or is a physical feature (hot). We could also attach to data access, bus access, they can have properties. Brendan – physical component, would be good. Mapping a variable for modeling. FACE has observables at an abstract level, then logical. Relating to the SysML physical modeling, they track to Modelica. ANSYS could contribute in this area. We are not trying to turn AADL into a physical modeling language but want accurate interfaces between the continuous physical and the discrete computer. Might impact the error annex, internal ports or observable. Compass had continuous time and Brian is looking into.
	+ Alexey, we may not want to separate the physical and logical so completely, the next instance of the system might transition from physical to logical.
	+ Physical vs logical – do we need another level of decomposition – Implemented As. Or containment of lower physical. Binding point groups – as a whole or as a part for binding memory for instance (Alexey).
	+ Do we have to have virtual memory? If it’s just a binding point vs the use of the physical and the virtual.
	+ Connectivity across the virtual platform, across virtual buses, virtual processors, virtual memory.
	+ Currently we use System to express the platform. Sometimes we might want a platform (Platform and Application). Pierre D.
	+ System can’t aggregate threads. We could allow threads but then would be the same as abstract.
	+ Physical could have subcomponent – so then it becomes like system. If you have physical feature do you need physical component. Need to hash out.
	+ Summary –
		- No nested processors, memory, buses: Composition via system
		- No virtual x as subcomponent of x: handled by bindings
		- Virtual platform with connectivity between virtual bus, virtual processor, virtual memory.
		- Composition through system component: no new platform category
		- Virtual memory and binding points: work examples to validate need for both
		- Features: non-directional, directional, bi-directional
		- Observable feature: for reasoning and for actual observation
		- Physical features: draft proposal of description and properties. Don’t reinvent but align with SysML and Modelica. Take a look at MILS/AADL continuous. **Action: Brian** 30 minutes in meeting.
		- Need a physical component? Nested physical component? Brian will include.
		- Binding-> allocation
		- Has bothered Peter:
		- Alignment of spec sheet for variants with component type? Do we need the implementation for …. Need an example **Action: Peter** will bring
	+ Processor provides cycles for execution, virtual processor for the scheduler.
* 1430-1530: Network Annex Draft Review and Update (Alexey Khoroshilov, Tiyam Robati, Brendan Hall)
	+ Draft available at gitlab.com
	+ Trademark – **Bruce Action**: Check with SAE
	+ Safety layer – they put another layer on top of AFDX, Brendan. Brendan has send around information. A layer above provides the interface. Recommend that we work out the interface, Brendan, Alexey, Peter, Steve in a
	+ Need to have the Guidelines for AADL annexes. It’s not the consistent.
	+ Need to add the generic properties for switched networks. Jerome has a set. **Action:** Jerome will send a set of generic properties.
	+ Honeywell can help on the TTA checked with TTTech. Send to Brendan with the former TTA properties.
	+ Safety layer – Brendan, what do you want to see? An generic example, a set of mitigation strategies to insure correctness, API’s for typical examples. Two CRC’s and a heartbeat. A white paper.
	+ Error model example is good to include. It could be reused. Now has an error model.
	+ Sections for particular protocols.
	+ **Actions**: Julien will send style guide
	+ **Actions**: Jerome will provide generic networking
	+ **Actions**: Steve – several additional properties they needed.
	+ **Actions**: Alexey provide to Brendan the current TTA definition for his getting a review.
	+ **Actions**: Get feedback – Jerome, Steve Vestal, Brendan, and Alexey.
	+ Then we would look at the error model annex and safety layer.
* 1530-1600: Break
* 1600-1630: Network Annex discussion continued.
* 1630-1700: SCADE AADL Capabilities (ANSYS)
	+ Hardware simulation combined with the software that controls it.
	+ Sim-explorer
	+ Configuration for FACE
	+ Configuration for AADL
		- Leverages the OSATE Analyses
		- We have WCET for SCADE code for specific architectures.
		- Ask about incremental analysis, integration of SCADE updates and AADL updates, they would like to discuss more.
* 1700-1730: Update on OCARINA (Jerome Hugues)

1) Develops a line of UAVs: fixed wings, quad copters, new projects

* + - * Incoming regulations to ensure safety during operation
			* Safety, scheduling and code generation, targeting Cortex-R
			* 2016Q4 new project to build analyzable AP brick (adaptable Auto Pilot used also by HACMS) using AADL
			* H2020 European project PERASPERA/ESROCOS
				+ With GMV as project leader, Nov 2016-March 2019
				+ Objective: develop extensions for TASTE towards space-qualified robotics applications, with variants: 18 month effort for Jerome.

Lab-Quality: regular Linus

Space-Quality: RTEMS for LEON3 + qualification materials

Impact on OCARINA – Qualification material to be produced

In-depth testing and analysis of code for major platforms

Ultimately, be embedded on space rover.

For TASTE not a lot of changes, new functional blocks, …

* + - * + Coupling AADL and FMI

Recurring needs to combine embedded architecture with physical environment in a rapid prototyping process.

Simulation of systems combining heterogeneous model is being standardized as part of the FMI standard.

* + - * + Coupling AADL and FMI

Code can be generated from AADL models for various RTOS’es

1, FMU as implementation for AADL devices

2, Turn AADL model into an FMU

3, Drive system-level simulation from AADL

Demonstrating all three together

Will be extended in another project to HLA potentially – distributed simulation. Combining FMI and HLA.

# Tuesday, Oct 4

* 0900-1030: AADL v3 discussions (Compositional Interfaces) (Peter Feiler)
	+ Review of concepts, has not changed from last meeting.
	+ Opportunity to update
	+ Composition of interfaces is a generalization of feature groups, replaces it.
	+ Composition aligns with extension
	+ System Receiver extends inverse of Logical, Physical -- inverse of only logical
		- Could use reverse
	+ Mapping - Missing an array interface, will get to when we get to arrays.
	+ Composition of modes – we currently do not support multiple mode states for a single component, would require only one mode state in a resulting composition?
	+ Remaining items – Arrays, Interface as concept/keyword
	+ Arrays – should be explicit at the architecture level. Roger. Brian-must have it when you create an instance model. Peter – we will do it at the configuration time. To be covered later in the meeting.
	+ You may need to configure the type as well as the implementation for array size.
	+ Power of 2, a constraint on an array.
	+ Out ports vs protocols on buses – our latency modeling takes this into account. Alexey, at the higher level, we think about how many elements are going out. Peter – that is platform dependent. It may be a shared variable vs queues, bursts etc.
	+ Pointing from the configuration to the implementation or the other way – the order impact the work in the AADL complier. Slide on Array Sizes provides the current take on the approach.
* 1030-1100: break
* 1100-1130: Continued (Compositional Interfaces)
* 1130-1230: AADL v3 discussions (array connections, unified type systems)
	+ Type System Unification
		- Get rid of aadinteger, just use integer. Was related to differences on target platform, but more than we needed.
		- Need to deal with Units, Alexey contribution, based on SI units,
		- Union of types
		- Sequences & Sets
		- Type conversion: explicit casting and implication for numeric – Real without .0 ok, numeric and numeric range (auto create range from first numeric)
		- Types like time: When to use integer vs. real.
		- Support for type inference from Value or type checking (Brian – much prefer checking)
		- Add map, graph, tree to aggregates which includes records, arrays, sets, list , sequences
		- Multiple implementations for type – Denis will write up some examples of use.
		- Type matching rules exist for classifiers. Issue of visibility rules for types vs. those for data classifiers.
		- Someone would like to be the driver for Meta Data?
		- Peter- do it in more than one step, like an onion, basic types first.
* 1230-1400: Lunch
* 1400-1500: Continued (array connections, unified type systems)
* 1500-1530: Break
* 1530-1600: Cheddar Update (Frank Singhoff)
	+ AADL Inspector & Cheddar – 1.6 coming out
	+ AADL Inspector – TL6
	+ AADL Inspector will have a translator from CAPULA to AADL
	+ New features from SMART (two year project from Brittany)
		- Define typical distributed/multiprocessor architectures AADL Inspector should support
		- How to model with AADL
		- Choose or design scheduling analysis features for those patterns.
		- Will Support partition scheduling and global queue of tasks distributed to multiprocessor. Partitioning supported in 1.6
		- Cache/CRPD-Aware Priority Assignment
		- Cache-Aware Scheduling Simulator
		- Networks-on-Chip (NoC)
		- Multi-Core – is really multiprocessor since most multiprocessor share buses and memory in various ways, you need to evaluate the specific architecture and capture it.
* 1600-1800: AADL v3 discussions (Configuration & Binding) (Peter Feiler, Alexey Khoroshilov, Denis Buzdalov)
	+ Choice points –
		- Subcomponent type-> implementation
		- Feature classifiers
		- If no choice points you can build an instance
		- Once configured, it cannot be changed.
		- Looks like an implementation, but it’s a final implementation
		- Prefer having the component category – Process configuration or System configuration rather than just the work configuration.
		- Choice points allow reaching down where prototypes did not but could use prototype name.
		- I always change (substitute into) the implementation.
		- Need to work the syntax, difficult to understand. Peter-I’m not happy with it yet.
	+ Denis White Paper
		- Is this a contract? Should some of it be outside the specification? Jerome. Which elements will provide what resources?
		- Denis – it’s a way to specify similar things in a similar way. More regular.
	+ Peter’s Bindings and Resources
		- Binding points or allocation points
		- SAVI wanted to map a functional architecture to a component architecture, we needed a new type of binding.
		- Use of resources goes beyond binding. Power Supply provides electrical resource, others consume it.
		- A power supply or a processor can have one binding point but many users of the resource. Can we have two binding points of the same resource and what would it mean. Would it be the some of the total things bound.
		- Binding point can be untyped, typed, constrained, with properties
		- One reason is so I do not have to reach down.
		- Another is to give greater freedom on how bindings would be done.

# Wednesday, Oct 5

* 0900-1000: Security Annex Discussion (Julien Delange)
	+ Domains – flight control vs entertainment
	+ Safety level – classification
	+ Encryption – logical separation
	+ Using ARINC as an example of separation
	+ On CMU-SEI GITHUB repository, see examples, AASPE
	+ Mitre rules – CWE are developed that fit with architecture and reusable Resolute verification provided based on this.
	+ Error types are mapped to CWE, such as CWE-349, from EMV-2 ontology defined.
	+ Graphic is used to show the relationships between error types
	+ Could put the tool that generated the graphic in OSATE perhaps for ontology displays
	+ Can use either code generator, the one for SEL4 or OCARINA
* 1000-1030: Discussion of SAE balloting process (Michael Thompson, SAE)
	+ Publishing Director
	+ How the end users interact – we publish in PDF
	+ Now convert into XML format
	+ How should we render your content.
	+ SAE MOBILUS is one platform, how to make more
	+ Can you provide the redline service for drafts
	+ David Alexander is working on tools for development of the standard.
	+ Video’s on how to apply the standard can also be provided.
	+ ARINC is part of SAE, available on some platforms
	+ If you complete the Word document, we build the XML
	+ David Alexander – working with IT to change the authoring tool
	+ LATEX – a typesetting language that is good for mathematics, almost all papers use.
* 1030-1100: break
* 1100-1200: AADL Core Errata (Peter Feiler)
	+ Userdays and Errata on the SAEAADL web site
	+ EMV2 - Semantics of XOR operator will be more complex. Will provide white paper recommending an approach to inform or auto transform, or keep the previous form.
	+ MASWIF ok with making the change, very limited use likely.
	+ Steve Vestal – **Action:** Peter will get back to Steve about where he can find his errata status.
	+ Switching between integer and real: Integer and real conversion: Implicit or explicit by casting. Real requires .0, if that is left out should we auto-convert? Requests for from JMR.
	+ Also numeric and range. Create a range if only one value provided if a range input is required. Request for from JMR.
* Bindings, Resources and & Layers
	+ Visibility of Binding Points
	+ Some users want the big level of memory, some what the data memory.
	+ Processor with a certain instruction set.
	+ Dependencies between them, some processor and memory requirements.
	+ Sam Proctor sending some examples of cross dependency on binding points
* 1200-1230: (1800-1830 Paris Time): EEA Brief Overview, and Translation of EEA to AADL and Simulation in AADL Inspector (Potential Presenters: **FranckCorbier/Garrett Thurston** from Dassault Systèmes & **Pierre Dissaux** from Ellidiss Software)
	+ Franck and Pierre primary contributors
	+ Scenario – integrating display units, to illustrate the value of using AADL to early allocation
	+ EEA is Electronic and Electrical
	+ Mapping is currently one way to AADL, could go back the other way. We just need to add the feedback way.
* 1230-1400: Lunch
* 1400-1500: Comments on Behavior Annex Ballot (Etienne Borde)
	+ Send\_result – is not working. Is it the plug-in or the standard that is the problem.
	+ Pierre D, the example is not correct.
	+ Will correct in the document.
	+ 1) accepted, added brackets
	+ 2) Change “will result” to “may cause” Not a big issue, keep it as it is.
	+ 5) Leave it as it is.
	+ Last one – For/forall – does not need to be changed. But an example will be provided to show it would not have to be an integer. Need paragraph to explain why it is a narrow set of circumstances– integer, event queue, array. **Action: Denis** will provide an example of interacting over a list of records with grammar definition.
	+
* 1500-1530: Break
* 1530-1630: Update on integration of BLESS/Formal Semantics with BA (Etienne Borde, Jean-Pierre, Brian Larson)
	+ Will be a BLESS Annex to keep it separate from the BA.
	+ Integrates BLESS and Jean Pierre formalizations.
	+ Working on a BLESS to Signal translator, within 95% complete. Would show demonstration model would show timing analysis with Polychrony and proofs with BLESS. For January meeting.
	+ Potential for Spring meeting informal ballot.
	+ AADL Runtime Service for Timeout
		- BA and BLESS have timeout as a dispatch trigger.
		- Should there be an AADL runtime service?
		- AADL defines a timed dispatch protocol with timeout:
		- Introduced as a means to have timeout without a timer.
		- BA has Wait\_For\_Dispatch
		- BLESS is very similar, just reset by events
		- BA and BLESS allow timeouts to be used for thread dispatch conditions.
		- Events on ports reset the timer.
		- These are part of the dispatch
		- For our purposes with BA and BLESS we only need time relative.
		- Intended to be V3, not 2.2
		- BA needs this.
		- Requesting that it be put in for V3 consideration.
		- Would like to support at the next meeting. Requesting some time to discuss. Should be compliant to POSIX timer – Frank
		- May be several timers, which one, what accuracy? We will handle it as errata for V3.
* 1630-1700: Planning for next meeting (Bruce Lewis)
	+ Sessions for the next meeting.

# Webex Info for the meeting:

Monday & Tuesday:

AS-2C AADL Committee

Every day, from Monday, October 3, 2016, to Tuesday, October 4, 2016

8:30 am | Eastern Daylight Time (New York, GMT-04:00) | 10 hrs

JOIN WEBEX MEETING

https://sae.webex.com/sae/j.php?MTID=mc418c5f09e3939a19ff96ef2644fcb68

Meeting number: 622 324 299

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: 622 324 299

Global call-in numbers:

https://sae.webex.com/sae/globalcallin.php?serviceType=MC&ED=487056622&tollFree=1

Toll-free dialing restrictions:

https://www.webex.com/pdf/tollfree\_restrictions.pdf

AS-2C AADL Committee

Wednesday, October 5, 2016

8:30 am | Eastern Daylight Time (New York, GMT-04:00) | 10 hrs

JOIN WEBEX MEETING

https://sae.webex.com/sae/j.php?MTID=m535925f4306857d353a1d189bb30b179

Meeting number: 625 457 830

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: 625 457 830

Global call-in numbers:

https://sae.webex.com/sae/globalcallin.php?serviceType=MC&ED=487057147&tollFree=1

Toll-free dialing restrictions:

https://www.webex.com/pdf/tollfree\_restrictions.pdf