AADL Meeting, Valencia Spain, Sept 29-Oct 2 2014

Attendees:

Brian Larson

Zhibin Yang

Jerome Hugues

Dominique Blouin

Tiyam Robati

Michael Lafaye

Etienne Borde

Pierre Dissaux

Frank Singhoff

Stephane Rubini

Denis Buzdalov

Alexey Khoroshilov

Bruce Lewis

Jean-Pierre Talpin

Huafeng Yu

John Preston

Nattias Nyberg

Jonas Wejtan

Total 17

-------------- Remote Attendees

Andreas

Ehsan Ahmad

Serban George

Philip Alldredge

Pierre Labreche

Steve Vestal

Ken Holmes

Dio de Niz

Total 8

Participating - 25

Bruce Lewis – AADL News and Issues,

Decision to move winter meeting 2015 to San Diego in Spring to hold down cost and to interact with the Open Group. **Action**: coordinate with Open Group, SAE, and Brazil - Bruce

Germany in the Summer was discussed as a possibility.

Draft Documents – Use the SAE standards work area, keep wiki area, provide documents through reference . **Action**: Bruce will look into, send link to everyone to look at.

**Action**: Bruce Slide with the list of tools – make it a table, could refer to wiki, update from the table on the Wiki with website links.

Tutorial for next meeting – RAMES also investigate Agree for future.

Another consideration - DASC Conference – Prague Fall, consider for Sept 13-17 as well as Models in Canada. Also Valencia is always a possibility (open invitation for any time).

Jean-Pierre Talpin - Synchronous Annex

Annex document provided. First draft.

Built from previous proposals.

Compound event replaced by a guard concept. Almost everything is in the proposal that we have developed so far.

Restrictions on guards and restrictions on behavior actions presented.

Need to add concept of oversampling. Will refine.

Planning an open source toolset building on the Behavior Annex. Not funded yet but could start in 2015.

Jerome - To make an annex, an implementation - Do we need to modify the core to add key words. Process abstractions should be put in processes/threads. Annex would contain the behavior abstraction then attach the behavior annex to the thread. The inheritance mechanism is meant to related abstract and concrete behavior. Would need to check formally to assure process and threads are consistent. Pierre D – no need to change the core language, add the constraint in the behavior annex. Could add constraints annex or use constraints within the SA. **Action**: Clarify how the behavior, constraint and SA work together and need to change Core for JP, with Pierre and Etienne, and Serban.

Etienne – modifications of the behavior annex, do you want your constraints to be a different, to not mix constraints and automata. Yes. About state machines? On guards. Non-deterministic automata.

Etienne – my suggestion, some aspects in BA as needed, those in first sections of draft annex, then restrictions go into SA annex.

Denis – Pre operator – when is it compared to zero (40). JP – not operational, just equational. During a given action, we would have these properties true. Denis – when is X=0, three alternatives. JP – during the previous action, x=0, then a must occur or d=1. When was the previous action? Assignment, write or dispatch? What is the time of the previous reaction. Its an abstraction, does not refer to any specific action. What we want to measure is the clock, each clock triggers action, an instance in logical time, its previous action. Refers to two instances in time, pre and current. Is the current complete state and a previous action.

Restrictions and consistency rules – (48) same concept a=0 is the previous action.

Real time constraints and logical constraints combined, over execution time. See (50) and (53).

Constraint specification means up to committee. Can be constraints from the constraint language. Need to discuss as a committee. **Action:** Need a recommendation from JP and Serban for the committee for how constraints would be best integrated.

Dennis – to the left is previous state, to the right the current state. But there seems to be a third in the sequence. JP – Yes, A=0 =>A=S3=>D=0 with D an input. It’s a causal implication. Error in (49) should be exactly 10 ms. JP – you are right, (49) (50) (53) should be corrected.

Loosely time triggered architectures – example describing the communication at (67), illustrated failed condition.

Correct (66) example.

Correct (68) example for output.

Rest of annex is basicly unchanged.

Dennis – need clarification on behavior inheritance in a thread. What can we do with inherited behavior and what not. **Action:** Discuss Inheritance with Dennis. JP – inheritance needs to be enforced perhaps by model checking or with an observer. Raise an exception if not performed.

Julien Delange - OSATE Update on OSATE

Supports AADLv2.1, plus behavior and error annexes.

Last month – code completion improvement in the editor, more completion by selection of available elements.

Outline (right pane of OSATE) improvements

Analyses improvement s - new latency analysis

Now testing each plug-in with regression tests, removed old Lute based 653 analysis, re-implementing to be more user friendly.

SEI blog post on AADL and Code Generation with OCARINA

Webinar provided which covers safety, latency, trade-off analysis, other analyses, includes the model that you can play with. Very well attended, 300 live online and over 100 reviewing after the Webinar. Model fully described on line on the wiki. Get web address from Julien.

Integration of graphical editor with updates of discovered bugs provided by UAH.

Good feedback from many on blog posts and podcasts – AADL has most popular blog post at the SEI, good for initiating people in AADL.

Ballot – Some had two user ID’s on SEI website, took time to resolve. If you have a problem, then contact Dorothy and Bruce.

Peter Feiler - Error Annex

Change to Error Annex - Added functional binding in Error Annex to support SAVI safety process and modeling.

Brings up a proposal for Version v2.2. Bindings – we consider bindings as an explicit part of the core language rather than a property. Allows adding new blinding types without a need to change in annexes.

Pre-defined state machines added from last ballot. These are available for use and extension. Four state machines defined with different failure mechanisms. Last case is for failure during recovery. Each is documented in the annex.

On capturing the condition that causes the error event. Using a string for now in the annex. Expression language to be defined later under v2.2. Like the property language, the expression language could be separate but usable in all annexes.

Synchronize with Constraints annex. Constraints will be static and behavioral.

AK - Property – impossible to refer to the property that is in a record. PF - We use a real number. We limited it to a fixed distribution. AK - Potential point for future improvement.

Peter – We already have a action item on “How do you specify a reference across the annexes and core. A standardized way to refer to objects in the model.

**Action:** Peter – will look at distributions that can be more general than a fixed distribution for error annex.

**Action**: Julien to develop proposal - For ballots in future, can we have the SEI send also the pdf as well as the word document? Some can edit into a pdf document. If you reply to the ballot in the document, then it should be easy to add comments at the point of interest and also enable editor to extract the information.

Julien Delange – 653 Annex

Pierre – comment to separate Annex into a time and space vs ARINC 653. Resolved: Julien will generalize the introduction and include an example like MILS. Also add text to describe use for mixed criticality.

Is it worth changing the textual use to A653, is a common way to specify ARINC 653. Resolved -If it impacts tools, its best not to make the change.

Next version of Annex should include part 2 (multi scheduling – modes) and 4 (single partition per thread subset).

Clarification: DAL property used as a consistency check for what is in the partition, as a minimum. Should add DAL property to the components as well so a consistency check can be made. At the type level it means no less than DAL permitted in the implementation.

**Action**: Check if Carnegie Mellon has a subscription to ARINC standards - Julien.

PL: Someone should participate in ARINC so they can get access to work in progress. SEI could subscribe for no fee to Apex (as university). ARINC standards now part of the SAE, so the SEI should be able to see work in progress. Called the IPC. You have a strong case for having access. **Action:** Julien will contact the lead for Apex.

Effort for next year – update for part 2 and 4. Don’t include multi-core yet since they are still working on their approach.

Jerome – renaming properties would resolve the issue of typing. Could be considered for v2.2. Sent email with the suggestions to Peter.

Dio de Niz – Analysis Contracts.

Developing with David Garlan, …

Started because of the number of analysis – many tools for control stability, scheduling, logic, thermal, power, aerodynamics.

We are all working toward multiple analyses in a single truth concept.

The problem is how do we put all the analyses together? Analysis assumption mismatches are discovered late in the system integration phase.

User cannot ignore the other forms of analysis, everything getting closer and closer together.

Systems getting more and more complex. Need to find a way to avoid mis-matches of assumptions and work together. Problem of integration of suppliers and models.

Very complex integration problem.

Our focus is automating the integrated analysis of important properties of the system.

Control domains provide continuous time but instant execution expectation. In conflict with the actual execution of the system. Time is required, processing loads, etc, AADL has been important in making this point. Example: Airbag deployed before the driver hits the dash/wheel.

Now have battery recharging via scheduler. Challenge is to integrate behavior related to charging, discharging from the car dynamics and effect in multiple cells. Battery heats up so Thermal Runaway Analysis to insure that it will overheat/cause fire. Cells separately monitored and controlled to avoid thermal run away.

Contracts talks about assumptions of the analysis and guarantees if met. What guarantees can the analysis provide. As an example, we need to be sure that two threads of high security/criticality are not on top of the same processor. So we put contracts on the analysis. When analyses interact, we need to create an analysis domain, an integrated set of analyses on a model.

We want to look at how the system will evolve over time.

Its analysis and synthesis.

We use various certifiers (model checkers)

Analyses are key for development of CPS, but inconsistent assumptions may compromise results,

Analysis contracts to automatically verify assumptions

Analysis contracts: sound and scalable. Without, single truth multi-domain analysis intractable.

Everyone complains about lack of semantics of simulink , but its in the way the user builds his specification, we would capture that in its own contract, we are not trying to build the hybrid model.

We have an implementation of this annex. Should be available soon.

Etienne Borde – Errata for Behavior Annex

Etienne recording detailed notes on each of the errata and the resolution, this just provides secondary backup.

D.3-05 - Second alternative to fix. This may be revised if Dennis provides an example to improve solution.

D.3-06 – add legality rule as specified in the first example.

D.3-07 – add a legality rule to make sure that transitions with otherwise as a condition are not priority

Extension of mode control for combinations of events – decided to do before, here is the example of use. Closed.

D4.04 – already approved in concept, here is the syntax proposal. At the mode transition level. Closed.

D.4-05 – what are the semantics? Is it just mode transistion or is it for other purposes as well? Used to raise an event to cause a mode change on an error in the core as the self event. Outgoing port can raise an event. Modify the syntax to allow internal events. Etienne – its just syntactic.

Will write a paragraph to describe, it will be in the ballot.

D.5.02 On the core side, input is frozen at dispatch. But in some cases we want to sample at a later time, this is supported but the statement on this is not clear. Dispatch or add legality rule that says that ports cannot be used for dispatch if input different than default.

D.5-03 Show example of use of the keyword. Complex topic. Will be summarized in Etienne’s notes. Enables control of which ports are frozen or none frozen. Works with the core specification.

Peter – ERRATA for Core

Changes to properties

* Latency, Actual Latency – added components usable with the property.
* Allowing period property on bus, virtual bus, (Brian - also consider an offset).

SEI property set – not part of standard but removed default value on Is\_Partition, Partition\_Latency

SEI property set used to provide properties to work with analysis methods supported in OSATE.

Inconsistent use of starting points in reference and applies to paths in case of subcomponent, proposal to fix is being worked on, affects only the connection binding.

Usefulness of Default value in Properties – currently default is that deadline is same as period, problem tools can’t tell if set by default or by user. **Action:** Peter requests all to look at the need for default value for properties. Remove default deadline =period

Frank – Default values – one could use the subset annex to create defaults, if not set by user, tool can set or can warn, as best decided by the analysis provider.

Peter – one can also set your own property defaults at the top and inherit.

Transfer of Aggregate Data. Can we treat it as a protocol. V2 is difficult compared to V1. Please interact with me on this. **Action**: Peter will write a white paper or email to propose a solution.

Name paths – for component hierarchy, Nested feature groups – need a unified syntax for paths from core or general expression into annex, or within annex start with core and back into annex. For next session, refresh the issue.

Thread: Duration and reserved port names. Issue Threads other than background are assumed to run infinitely. Proposed correction - introduce a Duration property, final port. Or could have duration on Modes. Its natural to chain together a sequence of these threads. Finalize is automatic. Dennis – does this work with aperiodic? PF - Sequence of 50 threads not easy to specify with modes. Pierre – want to be consistent with the BA when approach resolved.

* Abstract feature with classifier –
* Stack size for partitions – could be added to the virtual processor. Under consideration.
* Flows across modes – ok, but assess cost of implementation.
* End to End Flows Specification –

Special presentation on Variability – CVL and interest in AADL

Austin – overview of variability approach, working with OMG on a standard. Issue with patent holding up standardization.

BCL- an OCL lite weight Constraint Language

But you can use your own with tooling.

See paper <http://variabilitymodeling.org>

Tool being upgraded, will be open source.

Main problem – how do I decide to select a variation point over others, huge set of variability features (8000 in Rolls Royce, then 100,000s smaller variations)

See if selected features meet the features model constraints

If the prioritized quality attributes meet the constraints expressed with the impact relationships

If the realization meets requirements

Problems – we point to AADL with CVL. We need to do more to see how AADL will work. Is it possible you will work with us? (Yes)

Selecting subconfigurations.

Explicit representation of variability valuable to keep solving simple.

Basic model does not require that variability points are built in to the modeling language it is applied to but for architecture you need them to control correct construction. So in AADL we would want to use components and patterns of components, not breaking abstractions. Value for CVL approach is that analysis can be provided to evaluate the changed architecture. Value for AADL is that at a high level, AADL does not have to create a variability mechanism, if that is what we want. Variability control is already a part of AADL and we are considering extending what we have. More interaction of interest to both parties.

Alexey Khoroshilov : Network Annex

AFDX as defined in ARINC 664p7

Deterministic Ethernet – TTA

How much should be in the annex, target is that we could develop tools for the following use cases

Latency

, buffer capacity

, consistency – multi-level

, safety – may be later, Brendan working on.

, Synthesis and trade-off analysis,

 configuration generation – avionics switches etc.

Etienne – do you have classical configurations? Alexey – we support configuration for some cases in our tools already.

Synthesis – we specify high level requirements at the top level, we generate more details – virtual links and assignment. This synthesis.

**Action:** Jerome – we have training on these first two analysis, can provide

**Action:** Alexy – will mail an example of network with AADL, artificial example to include difficult issues, AFDX based.

Complexity – multicast, multiple partitions share one virtual link, internal and external buses … artificial example created to include the hard issues for specification.

Able to express now, for instance Multicast is a list of hardware components, better way will be discussed in AADLv2. (reference .., reference.., reference …)

Using virtual bus for virtual link

Bindings: using actual\_processor\_binding, actual\_connection\_binding

Brian – I will be excited to see what you provide, you are leading the way, for safety critical networks. ICE uses middleware that is similar to TTA. **Action**: Brian will send info on the ICE network on Ethernet to Alexey. **Action**: Bruce will see if he can contact Ramones (SP) at TTT. **Action:** Tiyam will contact Mirko, we should find out when we can brief them.

We will work on examples that have both TTA and AFDX. See what we can do in common and what needs to be separated in the outline of the document.

Peter Feiler – Roadmap Elements for v2.2

See notes from last meeting on the topics with assignments to some of the topics. **Action:**  Will need conference call to decide what to tackle for the next meeting – Bruce to initiate.

Usefulness of public/private package sections (Peter) – In 2000 we wanted package and public and private. But it seems to add unnecessary complexity to specifications. Users will probably control visibility through database access. We need a paper on, could put in the core as a note. Should check with SAVI. But **decided** that the private section of packages can be removed – Jerome, Etienne, Pierre, Alexey, Peter – developers agree, no exceptions except to talk to SAVI.

Inteface views

Health monitor only interested in a view of the interface. Jerome – I need this for code generation but we need to be careful of wording. Is it a concept of interface or a concept views? Serban – how does this differ from feature groups? PF – its not just the ports but other aspects too. Can I have a port be part of two feature groups, no. But ports can be in multiple views. Hardware view, software view.

Composition of features in views could be helpful to users. This is perhaps a good first topic of v2.2 for discussion at the next meeting.

Non-overlapping? Single name space is sufficient or overlapping with same feature in more than one view. Jerome – Example hardware – a pin but in software – a port.

Flows could only be constructed within a view if in the view contained them. But could still be constructed from the type and implementation of the full hierarchical model.

Composition of modes – composition of state?

Composition of Annexes in Views?

Feature group improvements

Virtual Memory component – mapping to an operating system and esp A653

Hardware flows –

Concept of binding – not hidden in properties, grammer or annex?

Unification of type systems & expression languages

Variability points and configuration

Arrays

State variables

**Brian Larson – BLESS updates**

Elie – Etienne’s student, working for AdaCore? Should become available for funded research. Open Do

Will send out for pre-ballot. Will put in an Eclipse help.

Expression language – very simple, works with X-text but took some work.

Supports virtual integration of medical devices, supports hybrid draft annex effort.

Supports high level safety and effectiveness analysis for the FDA. Need to be able to combine, interoperability support.

Ehsan – Hybrid Annex

Progress on Annex, some background

Motivation – many accidents have been caused by the controller

To be able to model the behavior of the device monitoring the environment with AADL.

First draft annex in July in Orlando.

Implementation of HA frontend for OSATE using BLESS

Isolette System – using the HA to model the air.

Sections – assert, invariant, variables, constants, channels, behavior.

Channels to specify communication channels.

See video for example

See annex for definition of terms.

Important contribution is the cyber-physical integration possible.

Have modeled three systems, grammar seems stable.

Movement Authority in Chinese train system.

<http://bless.santoslab.org> can download but just the frontend for modeling.

Need discussion on Activity instead of Process.

Most complex model is the isolate because the integration of the continuous and discrete.

Connection of the hybrid annex and the AADL architecture.

Remove behavior as much as possible.

Update HA with HHL prover.

Jerome – we need to see an example with interaction with AADL between the continuous activity and the AADL concept of thread dispatch and sensors. Eshan had an updated example of the train system. He can provide to Jerome and would like to discuss the what is needed.

Simulink to HCSP to Simulink

We will present the HCSP to Simulink.

**Dominique Blouin– Requirements**

Brian - RDAL was used to develop the documentation sent to the FDA. John Hatcliff is teaching a course. Don’t know if being used.

Peter Feiler – problem with associating requirements with models through the graphical view mechanism, not efficient, too many windows to use. Some are part of the system, some are on the system. We used it for a class with AADL. Several use scenarios – new development or existing documents to bring into the framework. Need to get and push to Doors. We want to flesh out the evidence of correctness part of RDAL. We want an incremental assurance case approach and have a project to do. When doing the textual experiment we did not stay very close to the meta-model.

Brian - General technical requirements – general principles that apply to all systems in a class of products. Stakeholders vs system requirements. PF-How to design to help user? Stakeholder requirements are typically goals. Multi-level step to get to the requirement. DB-Every requirement had to have a reference into the architecture.

DB – textual needs to be worked next. Issues on releasing the sources with the University. We will put the source on get-hub since nothing else seems to be working.

Goals versus requirements

With Clauses – to enable import

Traceability –

Changes for assurance cases modeling

What is needed for ballot? Over the next year we can get these things resolved. DB-I agree. PF – project just started, we should have the input.

Etienne – I’m using it to express goals. Glad to see it on Get-Hub.

Etienne Borde – Behavior Annex Continued.

D.5-04 - We need a white paper with rational and examples to decide if we make the change. Denis would provide.

D.5-05 – Accepted.

D.5-06 – Is a core issue related to output queue. We do not have a queue on output, but a single value. Will need to think more about this.

D.6-02 – Could be done but could ask for the syntax, but it is a compaction. Before you freeze you have the old value, when you freeze, you have the new value, can you get an indication of direction of change. Result – since you can do it without the new feature by preserving the last value it does not need to be added.

D.6-06 – OK

D.6-07 –

D.6-08 – OK, closed.

D.6-09 – Ask for rational from Mamoun

D.7-02 – relates to units. Add a paragraph limiting the use of property association to properties without units or with limit units, should be changed after publication of v2.2 with units annex content.

D.7-03 – add a paragraph and make sure it exists for behavior condition and behavior actions.

G-03 (1) Investigate libraries for BA like EMV2

G-03 (2) closed, rejected.

Completed review of BA errata suggested. Now can work toward ballot of upgraded Behavior Annex.