SAE Architecture Analysis and Design Language

AS-2C AADL Subcommittee Meeting

May 2-5, 2016

Chattanooga, TN

AADL

Upcoming SAE/AADL Meetings

Spring 2016 – Chattanooga, Tennessee, May 2-5

Tuesday nite boat ride starting at 6:30. Staying over Thursday? Shuttle to aquarium.

Summer 2016 - Fourth week of July, July 25-28. Thomas Noll is sponsoring at the RWTH Aachen University. Fly into?

Fall 2016 – Our meeting Oct 3-6 at the SEI.

Embedded Systems Week in Pittsburgh, USA Oct 2-7. (International Conference on Compilers, Architecture, and Synthesis for Embedded Systems, International Conference on Hardware/Software Codesign and System Synthesis, International Conference on Embedded Software). Abstracts April 1.

Julien – coordinating workshop with Tucker Taft on Architecture. Details?

Winter meeting - Someplace warm? Nice?

AS5506 AADL Standard Status

- SAE standard AS5506 Architecture Analysis & Design Language published.
  - Nov, 2004.
  - Jan, 2009 . V2 Published w Graphics Annex http://www.sae.org/technical/standards/AS5506A
- SAE Annexes AS5506/1, June 2006. Includes Annexes for Graphics, Ada & C Programming Guidelines, Error Modeling, Meta Model
- SAE Annexes AS5506/2, January 2011. Includes:
  - Behavior Annex, Data Annex, ARINC 653 Annex
- SAE V2 AS5506B, Published, Sept 2012.
- AS5506/1A, Published, Sept 2015 – Annex A: ARINC653 Annex, Annex C: Code Generation Annex, Annex E: Error Model Annex
- SAE V2.2 AS5506C, Ballot ready to be started.

AS5506 AADL Standard Roadmap

- Next =>SAE Annex AS5506/2A Includes: -- Annex B - Behavior Annex, Annex D - Data Annex, (ARINC653 was added to 1A).
  - Add to 1B or use 2A to keep separate
  - Formal finished by for July meeting?
  - Complete for Pub Oct 2016
  - Etienne – is there a better way to do this, like individual annexes

- New Annex - RDAL, Constraints, Subsets, Network Annexes, …
  - Add to AS5506 /2A as 2B. Limits number of documents users need to buy.
  - Informal on constraint by July 2016 , draft of Network Annex
  - Formal ballot when?

- Update AADL Core to V3.0 AS5506D - Peter has started to write, target for?

AADL WG Activities

- Requirements Annex (80%) => Peter has textual and assurance case capability in OSATE, should we combine?
- Constraints (Analysis) Annex (80%) - (Serban) Final draft before July? Would requires coordination meetings to achieve, so we can have informal.
- Update Behavior Annex (100%) (Etienne, Pierre D, Jean Pierre, Brian Larson). Ballot BA, then integrating formal extension to Annex (JP), Ready to ballot?
- Constraints to be presented in draft at July meeting.
- Network Annex – (60%)(Alexey, Steve Vestal, Brendan Hall Tiyam …)

  Need draft if ready, people will use it for guidance and give feedback.
- ARINC 653 Update to new ARINC for Multi-Core with Part 2 and 4. (Julien, PL, Alexey) Later? what is the status of need in industry?
- Data Annex (95%) (Jerome) => Some work on Data annex and experiments with code generator needed to finalize. So are we expecting re-ballot on code generation?
- Others .. Hybrid (still active?)

AADL Annexes Being Developed and Brought to Committee

- Some annexes should be published, some will be developer provided and widely used without publication as part of the standard. Problem of complexity, redundancy, maturity, tool availability …
- Hybrid Annex – Ehsan Ahmad, Brian Larson – Need something but not a new language to express differential equations. Need the interface from world to system. Interface to to Modelica. Brendan and Brian. May be better to have something like the code generation annex. Defining bridges. FMI wrapper for AADL. OCARINA will have an FMI export. Need additional cyber-physical analysis approach.
- Jean Pierre, Fredrick Mallet – Nice, considering how continuous time can be added. Fredrick willing to sponsor meeting in Nice.
- Rockwell – need behavior side of the constraints annex. This is later.
- Peter's question – should we make presentations public, keeping drafts private on the SAE website.

Tutorials for User Support

- Tutorials to date: BLESS (Fort Lauderdale), STOOD (Orlando), Paris (ASIIST), Toulouse (Compass), Toulouse (TASTE), Minneapolis (FUSED), Valencia (RDALITE), Jacksonville (BLESS Isolette), Montreal (MASIW), Santa Barbara (AADL Inspector 1.3), Orlando (OSATE Safety), Valencia (TASTE), San Diego 1&2 (no tutorial), Madrid (MASIW), Seattle (used for V3 discussion), Toulouse (No tutorial), Germany (MILS w std AADL or ?), Pittsburgh (workshop)

Potential for future meetings:

- OSATE/OCARINA – Delay until Winter of 2017?
- RAMSES – Etienne – Summer of 2016?
- Using BA with Polychrony/BLESS – Jean Pierre, Brian Larson - Fall of 2016?

Joint Research

- Projects contracted for FY14, 15 on Code Generation and Constraints, health monitoring for 653.
- Constraints Annex FY15
- Now considering next phase.
- Potential for additional projects where we can advance research if funding available.

AADL

Planning for Summer 2016

- Possible User ½ Day
  - D-MILS tutorial (2.5)
  - OCARINA for Multi-Core (1)
  - Timing (Fredrick Mallet) (1)
  - Total 4.5 hours

- Standardization
  - News (30 min)
  - AADL V3.0 topics PF (8 hr)
  - Errata Core PF (1.5 hr)
  - Errata BA EB (1.5 hr)
  - Integration of BA with BLESS/Sync (2 hr)
  - Errata/Update Data Annex (30 hr) (JH)
  - Constraints Annex SG (2 hr)
  - Next Meeting Planning and action items (30 min)
  - Network Annex Draft (Alexey) (2 hr)
  - Total 18.5 hours

- Additional topics
  - Hybrid Annex - Simulink/Scade AADL Integration with Example (Ehsan, Brian) (1 hr) min)
  - Requirements Annex - RDAL/AADL/Textual, Assurance Case Update (Peter) (2 hr)?

Actions

Action	Date	Lead	OK
Check with Thierry on 653 update (answer - part 4 should be incorporated, part 1 has been updated, later part 5 on multi core) (interest in adding health monitoring (Etienne), more dynamic parts)	3/13	BAL	X
Schedule with Frank for Stephen Presenting (Cheddar, 653 scheduling, patterns, subsets, multi-core)	3/13	BAL	X
Track Analysis updates in AADL Inspector	3/13	PD	X
Update White Paper on Synchronous Annex	3/13	JPT	X
Contribute to Synchronous Annex White Paper (methods)	3/13	JH, BL	X
Update on platform independent code generation and medical domain research (TIMES)	3/13	OS	
Post bimonthly SEI AADL Modeling Forums on AADL, results to be captured	3/13	JD	X

Actions

Action	Date	Lead	OK
Contraints (Analysis) Annex – 4 hours for Montreal	3/13	SG	X
White Paper on referencing objects in Declarative and Instance model in OSATE (Eclipse)	3/13	PF with DB	X
Requirements Annex – add definition of contract term usage	3/13	DB	
Send DB Mike Whalen's requirements presentation	3/13	BL	X
EM2 properties concern to be documented	3/13	JH	
Example of explicit propagation with masking to show limited propagation for EM2	3/13	PF	
Discuss Multiple approaches proposed for Unit Relations and Basic Expressions for Unitful Values	3/13	AK, JH, BL	X

Actions

Action	Date	Lead	OK
Code Generation Annex – two different mappings for subprograms, call sequences, need clarification on data flow	3/13	JH, PD, PF	
Code Generation Annex – legacy component interface integration property	3/13	EB, JH	
Multi core representation guidance needed, set up discussion and write white paper	3/13	JD, S Rubini	X
Set up discussion on Multi-Core – 3 hours for Toulouse	3/13	BAL	X
Lead discussion on Multi-Core	3/13	JH	X
Recommendations for improving consistency of AADL symbols, also behavior and error model representations Toulouse 1 hour	3/13	PF	
Errata – need to discuss dependency across annexes and whether a coupling annex is needed instead of self Event	3/13	PF	

Actions

Action	Date	Lead	OK
Errata – discuss Flows and Modes for fault tolerant support	3/13	PF	
Errata – discuss Contained property associations with Annex fragments	3/13	PF	
New annex suggestion: ARINC 664 guidelines, Alexey to present his approach at Sept Meeting	7/13	AK, BH	X
Possible annex - FACE interface Confirm with BH if he can present concept at Toulouse Meeting.	7/13	BH	
Subset and Constraint Annex Coordination	7/13	SG, VG, JH, AK	X
Constraints Annex – Can we place contraints on use within a component or where? AK	7/13	SG	
Functional Hazard Analysis name fix in documentation of safety tools in OSATE	7/13	JD	

AADL

Actions

Action	Date	Lead	OK
Update Isolette example model on wiki	7/13	Brian L	
Add regression test suite to OSATE release mechanism	7/13	JD	
Provide Adele/OSATE synchronization prototype	7/13	DB	X
Provide experience report with Requirements Annex in Sept	7/13	Brian L	
Provide simple example in Requirements annex extendable to goal example	7/13	DB	
Start development of white paper (comparison) and possible draft for Unitful Conversions for Sept	7/13	AK with BL, JH	X
Explicit vs automatic conversion of units example	7/13	AK	

AADL

Actions

Action	Date	Lead	OK
White paper on multiple bindings to hardware (M Core. Mem) to see if we can improve approach we are using now.	7/13	PF	
Review upgrade needed on 653 annex based on Part 4, developing part 5.	7/13	JD	
White paper on nested feature groups, mini annex recommend	7/13	PF	
Textual syntax for requirements annex – Sept (Brian will give it a try, Peter working on, European project)	7/13	Brian L, DB, PF	
JD will package up Bella Padula for OSATE2	7/13	JD	
Alexey, Peter, Dominique, Pierre L, Jerome to study the issue of updating the core vs annex in relationship to units, unit type, and the property language, to bring a recommendation for Feb, 2013	9/13	AK	X
Dominique to present SysML units approach and experience using.	9/13	DB	

Actions

Action	Date	Lead	OK
Etienne, Jean-Pierre T, Pierre D to develop recommended update to behavior annex with regard to synchronous annex behavior for Feb Toulouse meeting.	9/13	EB	X
Jean-Pierre, Serban to evaluate use of PSL to express synchronous annex constraints for Feb Toulouse meeting.	9/13	JPT	X
Etienne to review Errata for Behavior Annex at Feb meeting in preparation for a revision to annex.	9/13	EB	X
Vincent will provide draft subset annex for Feb meeting	9/13	VG	X
Peter will provide draft of error annex for informal ballot, mid November, to be returned mid Jan, for Feb meeting resolution	9/13	PF	X
Add link to OSATE help for making bug reports	9/13	JD	X
Alexey and Jerome will provide an overview of the approaches for specifying AFDX and recommendations for other buses that we might want to provide guidance for specification and analysis.	9/13	AK	

Actions

Action	Date	Lead	OK
Jerome will provide a recommendation for supporting interrupt events for Feb 2013 meeting	9/13	JH	
Create a list of benefits/issues related to using SysML vs RDAL for requirements	9/13	DM	
Brian to present SEI work for Feb Meeting	9/13	Brian L	x
Provide time for PG Polarsys presentation for Feb Meeting	9/13	BAL	x
Schedule presentation with S18 of the safety analysis tools	9/13	BAL	
Standard properties for tracing requirements to components in RDAL	9/13	DB, PF	

Actions

Action	Date	Lead	OK
Present Multi-Model Traceability Language by Open People	9/13	DB	X
Present new work with BLESS done with the SEI	9/13	Brian L	X
Mapping of a persistence property for consistency analysis between input and output, must match for consistency	9/13	Brian H, PF	
Check – composite error model at the composite level can have incoming propagations that do not impact subcomponents	9/13	PF	
Function binding to components so errors at component level can fail function and hazard analysis bottom up	9/13	PF	
Brendan – we want “refines to” in the syntax	9/13	PF	
ARINC 653 has Multi-Core working group – contact TC	2/14	JD	

Actions

Action	Date	Lead	OK
What timing/performance for processors should we support – reference, measure, mips? Peter to provide slides.	2/14	PF	x
653 timeout associated to ports – do we need a timeout port property to wait added as part of the Core. Alternatives?	2/14	PF, JD	
Publication permission for Joint research reports	2/14	JP, BAL	x
Splitting 653 annex properties into two parts, second for implementation dependant. Need errata?	2/14	JD	
Request for Peter to give a presentation on FMEA and the stepper motor.	2/14	PF, BAL	
Dominique to study Peter's recommendations (slides) and tech report for RDAL, Jerome as some related activities	2/14	DB, PF, JH	
github for version 2 of RDAL needed	2/14	DB, JD	

Actions

Action	Date	Lead	OK
Dominique to present gobal model management	2/14	DB, BL	X
RDAL textual syntax – send to Peter what you have	2/14	DB, Brian L	
Error model annex - Provide summary of how the core error reporting and annex errors interrelate.	2/14	PF	
Error annex issue of terminology in different domains – write up guidance for understanding.	2/14	PF	X
Given write up on terminology - ask Alex Boydston, PL review	2/14	BAL	x
Need config file description for VxWorks, new ARINC653 standard, see if available.	2/14	EB	x
Virtual buses and processors – Investigate end to end flows in the hardware and the containment and connection of virtual buses.	2/14	PF	

Actions

Action	Date	Lead	OK
Concept of treating the core as two languages, the architecture and properties. References should be available throughout model space.	2/14	PF	
Unit types - Need to express evaluations that have a formula. Modelica as an example.	2/14	AK	
Flesh out additional rules for “implemented as”	2/14	AK, PF	
Recommendation for laying out virtual memory	2/14	AK, PF	
Uniform way to do compute from different contexts	4/14	PF	
Email to S-18 about Chicago and San Diego (Julien Chicago?)	4/14	BAL	x
Develop predeclared error behavior state machines for Annex	4/14	PF	

Actions

Action	Date	Lead	OK
Provide contacts for textual RDAL at Cantabria	4/14	DB	
Provide textual RDAL ideas, examples to Peter	4/14	BLarsen, DB	
Provide example large assurance case to Peter and Dominique	4/14	BLarsen	
Provide papers on verification task to Dominique	4/14	PF	
ARINC653 update to style used in BA with traceability	4/14	JD	
RDAL needs concept of negative requirements	4/14	PF	
Send email to chair of S-18 for Spring Meeting	7/14	BAL	x

Actions

Action	Date	Lead	OK
Start second ballot for Error Annex with Code Generation	7/14	JD, BAL	x
Discuss doing Julien's AADL webinar for upcoming meeting	7/14	BAL	x
Request TASTE tutorial for Valencia	7/14	BAL	x
Interaction between BLESS, Assertions and Agree, set up discussion.	7/14	BAL	
Telecon to start network architecture discussion and determine presentation	7/14	AK	x
Add pre-defined error state machines to Error Model Annex	7/14	PF	
Send Peter a list of variations in exposure time, ARP 5107	7/14	BH	

Actions

Action	Date	Lead	OK
Contact Bill Flecher and Brendan Hall for uses of “Time Limited Dispatch for EA	7/14	PF	
Contact Darren Cofer to get input on security types for EA	7/14	BAL	
How is SysML handling having one link that goes two places, a multicast link.	7/14	BH	
FACE data modeling for integration into a partition, send code generation annex to the data modeling group	7/14	BAL	
Update the ARINC653 annex for the next ballot	7/14	JD	x
Schedule a demonstration of AADLlite using Subsets Annex	7/14	BALS	
Sets vs lists – provide example of when needed	7/14	AK	

Actions

Action	Date	Lead	OK
Coordinate with Open Group, SAE, Brazil for San Diego mtg	10/14	Bruce	x
Draft Documents on SAE standards work area, keep wiki (should do with a link to the wiki on SAE site)	10/14	Bruce	
Table of tools and website links (link to wiki)	10/14	Bruce	
Synch Annex - Open Source toolset building on Behavior Ax	10/14	JPT	
Synch Ax – Clarify impact on core, behavior, constraints Ax	10/14	JPT	
Synch Ax RT and logical constraints integrate, constraints Ax?	10/14	JPT, SG	
Synch Ax – clarify inheritance of behavior in a thread	10/14	JPT, DB	

Actions

Action	Date	Lead	OK
Error Ax – expression language useable on all annexes	10/14	PF	
Error Ax – distributions more general than fixed	10/14	PF	
Future ballots – can we also send and edit PDF as well as Word	10/14	JD	
653 Ax –generalize intro to cover MILS, mixed criticality	10/14	JD	
653 Ax – Check if Car Mel has subscription to ARINC stds	10/14	JD	
Analysis contracts – update committee on implementation	10/14	DD, JD	
Errata for core – inconsistent starting points for paths	10/14	PF	

Actions

Action	Date	Lead	OK
Errata for core – Usefulness of default values	10/14	PF	
Errata for core – Transfer of aggregate data as a protocol?	10/14	PF	
Errata for core – name paths need unified syntax	10/14	PF	
Net Ax – provide training example of two network analyses	10/14	JD	
Net Ax – provide ex AFDX net architecture difficult issues	10/14	AK	
Net Ax – provide example ICE network, similar to TTA	10/14	BL	
V 2.2 – usefulness of private package sections, check w SAVI	10/14	Bruce	

Actions

Action	Date	Lead	OK
Hybrid Ax – need example cont time vs AADL thread dispatch	10/14	Eshan, BL	
BA – need white paper to change D.5-04	10/14	Denis	
BA – D.6-09 – ask for rational from Mamon	10/14	EB	
Verify that last ballot passed.	2/15	BAL	
Redefine Ballot Pool	2/15	BAL	
Integrate document for publication	2/15	JD	
Resolve BLESS issues with Core, BA, and Code generation	2/15	BL	

Actions

Action	Date	Lead	OK
Provide network (TTE, 664) properties and links for scheduling, safety protocols	2/15	BH	
Open group - Formalized Assurance Cases – DEOS runtime monitoring - assurance in safety and security	2/15	BAL, PF, Rance D, Joe B	
Synch/BA - Immediate connection to data ports only vs queue of one, should we allow both?	2/15	PF, EB, JP	
Constraint Annex – Review actions relative to control of execution of theorems for testing and assurance cases	2/15	SG, PF	
Constraint Annex – “applies to” at the theorem or viewpoint	2/15	SG, PF	
Constraint Annex – send to Mike Whalen, Brendan Hall	2/15	SG	
Constraint Annex- review relationship to assurance case, behavior, simplification, relation to RDAL	2/15	PF, SG	

AADL

Actions

Action	Date	Lead	OK
Graphics-need graphical specification of flows and flows for error propagation, color coding, ability to tweak autolayout	2/15	PA	
Requirements – issue between X-text and Extend, need to develop best infastructure, may impact OSATE, RDAL	2/15	PF, EB	
Provide pointers to create references into the use case	2/15	DB	
Error Model – note to be provided that gives examples of exposure time and exposure instances,	2/15	PF	
Error Model – map two examples of communication between annexes. AADL vs SLIM	2/15	BH	
Error Annex interaction with Behavior/Hybrid Annex. Set up time to discuss at next meeting.	2/15	BH, PF, BL, PD	
EMV2 elements are inherited and can be overwritten, but not documented in EMV2 text	2/15	PF, AK	

Actions

Action	Date	Lead	OK
5506B has been updated on wiki for two years, need to update document.	2/15	PF,	
Migrate SEI properties to property sets reflecting purpose, All send what you think is useful.	2/15	PF	
Recommendation on properties for internal features	2/15	PF	
Multi-core processors – develop white paper on nesting of processors if needed.	2/15	JD	
Multi-Core – leave for V3.0 discussions.	4/15	AK, JD	
Data Modeling Annex – add processor types like endianness	4/15	JH	
Data Modeling Annex – provide bit stream example, work text with Bruce, expressions in property strings	4/15	JH	

Actions

Action	Date	Lead	OK
Add time stamp property to Network Annex.	4/15	TR, BH	
Scheduling protocol inherit list with defined semantics	4/15	PF, DD	
Arrays with another input form so you can copy and paste	4/15	PF	
Brendan requesting early draft of synchronous updates to BA	4/15	JP	
Myron will see if he can provide example of processor synch	4/15	JP	
Conditional And, Or support in the BA – need to make it precise	4/15	EB, BL	
Functional invocation needed in the BA, Brian will provide example	4/15	BL, EB	

Actions

Action	Date	Lead	OK
BA – Assignment of Any – Brian will check with Mamoun	4/15	BL	
BA- Subprogram Invocation – consider further	4/15	EB	
All, send BA comments to Etienne, Pierre will test syntax	9/15	EB, PD	x
BA must sense error and raise it, need example, define semantics for this internal event	9/15	EB, PF	
Etienne, Brian, JP to work BA integration, JP building a tool environment Quegen over next two years, Formalization target async, sync and timed systems	9/15	EB, BL, JP	x
Short term – skeleton for BA, longer term merged semantics	9/15	EB, BL, JP	x
Peter to all, virtual contains channel and protocol, please provided why we need both channel and virtual bus	9/15	PF	

Actions

Action	Date	Lead	OK
	6/15		
	6/15		
	6/15		
	6/15		
	6/15		
	6/15		
	6/15		

AADL

Actions

Action	Date	Lead	OK
Brendan to have webex with Peter, Pierre to explore the suggested array solutions.	9/15	BH	
V3 - Peter to determine if we can do state machines aka state variables	9/15	PF	
	6/15		
	6/15		
	6/15		
	6/15		
	6/15		

AADL

BACKUP

Focus for tools and analysis

AADL tools – Graphics (Dominique +), Robustness (Julien, Peter), Large Scale Models, integrated generation for safety critical/robust systems (Etienne/Jerome), integration across toolsets/analysis (STOOD, Dominique +), Ease of use (Glasses), Documentation (STOOD),

Analyses –

Have – 4761/6110 safety analysis (new), security, latency, processor and bus utilization, scheduling, I/O channels (ASIIST), generation, domain specific graphical front ends, 653 constraints, 653 scheduling (new) (Cheddar), simulator (AADL Inspector),

Need – ease of integration, ease of use, pre-integrated, analysis extensions for complex distributed, formal analysis (constraints/sychronous), 653 Generation, etc.

AADL Tool Integrations

Frank Singhoff - AADL/Cheddar – through Ellidiss, TASTE, and OCARINA

Jose Mesquer - AADL/MAUDE –

Jean Pierre Talpin - AADL/Polychrony/Signal

Pierre Dissaux - Ellidiss - AADL/Domain System Engineering - Graphical STOOD, Adele, GLASSES, Analysis AADL Inspector, Simulator, Behavior Annex, Error Annex, Requirements Annex.

AADL/Real, Lute, Agree – Integrated in last release of OSATE by Julien

Brian Larson - AADL/BLESS –

Etienne Borde - AADL/Behavior Annex, RAMSES

Dominique Blouin - AADL/Requirements Annex and Adele to OSATE upgrade

AADL/Compass – safety, uses a subset of AADL, also extends the subset.

Peter Feiler, Julien - AADL/SAVI – Updated for V2, extended, new analyses for Safety (FHA, FMEA, Reliability, FTA, Prism) , Simulink to AADL and reverse.

Jerome Hugues - AADL/Mast/Cheddar/… as part of OCARINA Generator

Alexey Khoroshilov- AADL/MASIW – Modular Avionics System Integrator Workplace, plus verification tools.

Rockwell Collins – SysML to AADL, Lute, Agree, Resolute, Spear, QuasiSyn…