

# SAE Architecture Analysis and Design Language

AS-2C AADL Subcommittee Meeting

Nov 5-8, 2018

London, UK

# Upcoming SAE/AADL Meetings

**Fall 2018 – SAE London, Nov 6-8, Aerospace Systems and Technology Conference, (ASTC). Paper submission deadline May 20.**

**Winter 2019 - Feb 12-18 2019 Georgia Tech, confirmed as specified at the last AADL meeting.**

**Spring 2019 – June 10-14 Paris – ParisTech (week before Airshow)**

**Fall 2019 - Sept-Oct US - Grand Canyon in planning by ASD?  
~~AeroTech Bordeaux 23-26 Sept~~**

**Winter 2020 – Jan 2020 Toulouse with ERTS.**

**Spring 2020 May/June Minneapolis**

# AS5506 AADL Standard Published

- SAE standard AS5506 Architecture Analysis & Design Language published.
  - **Nov, 2004.**
  - **Jan, 2009** . V2.0 Published w Graphics Annex  
<http://www.sae.org/technical/standards/AS5506A>
  - SAE V2.1 AS5506B, Published, **Sept 2012**
  - SAE V2.2 AS5506C, Ballot completed, Published **Jan 21, 2017**
- 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.
- AS5506/1A, Published, **Sept 2015** – Annex A: ARINC653 Annex, Annex C: Code Generation Annex, Annex E: Error Model Annex
- AS5506/3 - Behavior Annex, published **Aug 2017**

# AS5506 AADL Roadmap

- We now have permission to have separate annexes and they will be bundled to make them more affordable. The annexes could be a bundle.
- Behavior Annex is AS5506/3.
- Network Annex near ready 5 – Ready to start informal ballot for Feb 2019?
- FACE Annex AS5506/4 - Review informal ballot results.  
[www.adventiumlabs.com/camet/face](http://www.adventiumlabs.com/camet/face)
- Security next – 6? Informal May 2019?
- Update AADL Core to V3.0 AS5506D - Upward compatibility needed with translator, if downward compatibility possible, should consider. Needs to be stable as well with translator from 2C, both maintained for a while. Fall 2019
- ARINC 653 Annex, will depend on AADL V3 multi-core, 7
- Data Annex is waiting for AADL V3, 8, depends on units,
- Code Generation Annex after AADL V3, depends on runtime also, would be 9
- Updated EMV3 with integration with Behavior Annex (cross dependancy)  
Now have internal ports between annexes. Need example to show how to use ports. Example could be an AIR.
- Formal Behavior – update to 3, would it be 3A
- Upgrade to runtime services now, is that against 2.2 creating 2.3 or 3.0?
- AADL Workflow Guidance Document (include SysML high level). Need volunteer, start is Jerome's presentation for this meeting/conference.

# AADL Working Groups

- **Requirements Annex to become Assurance Annex** ( 50% ? ) => Peter has textual and assurance case capability in OSATE, planning to combine with Requirements Annex. **Post V3.**
- **Constraints (Analysis) Annex** (50% ?) - (Open Lead) First draft provided but not enough consensus to carry forward. Includes OSATE compatible toolset to specify. **Support Assumes/Guarantees?**
- **Behavior Annex Updates** (Etienne, Pierre D, Jean Pierre, Brian Larson). Completed. Next phase w formal annotations (behavior constraints) sub annex. (EB, JP, BL) **after study of runtime services.**
- **Network Annex – (80%)(Alexey ...).** **Should/could have general section for network properties?.**
- **ARINC 653 Update to new ARINC for Multi-Core with Part 2 and 4.** Update when multi-core expression standard ready as part of V3. Steve Vestal, Alexey?
- **Data Annex (95%) and Code Generation Annex (Jerome)** => Some work on Data annex and experiments with code generator needed to finalize. Reviewing runtime services this meeting and current issues.
- **Security Annex (40%)– Dave Gluch .**

# 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.
- [FACE Annex proposed by Tyler Smith, 3rd draft result of informal, ready for formal?](#)
- [Jerome suggested other AIRs](#). Safety AIR 4754 and 4761, integration with system engineering. AIR by S18 AADL equivalent. Paper by SEI on safety could be converted to an AIR. [Guidance for SysML/AADL Integrated Use](#).
- Hybrid Annex – On hold as we consider need. Need the interface from world to system. Interface to Modelica. Brendan and Brian discussing. May be better to have something like the code generation annex. Ties to time domain.
- STPA and AADL – tremendous opportunity from EMV up and down abstraction levels. Related to Security annex. [Could be an AIR, who would lead?](#)
- Exploring FMI wrapper for AADL. OCARINA will have an FMI export. Adds an additional cyber-physical analysis approach. [May lead to annex or AIR](#). FMI also being worked by Ellidiss. Jerome Hugues.

# 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 (will be the two day workshop), Toulouse (ALISA), Atlanta (OCARINA), Fort Worth (attend conference), Pittsburgh (Adventium tools) [London \(RAMSES\)](#) *So many possible, may need workshop.*

Potential for future meetings:

- Cheddar and Ellidiss STOOD/AADL Inspector
  - FACE, SCADE Integration w AADL ANSYS
  - [Specific AADL Analysis tools](#)
  - MASIW
  - TASTE
- 
- [We should add a workshop day or two to a meeting, could do it in Atlanta? Ideas for how to do it?](#)

# International Joint Research

Suggestions:

Targeted for European research groups

- Seamless refinement from SysML requirements/functions/behavior.
- Tool Certification related
- Analysis compliant code generation
- Multi-core
- Cyber security analysis



# Planning for Feb 2019

- Possible User ½ Day
  - Trade-Space SEI (30min)
  - Safety and Security Assurance LAMP (P. Dissaux)
  - ...
  - ...
  - Total 2.0 hours
- Standardization
  - News (30m)
  - Next Meeting Planning and action items (30m)
  - AADL V3.0 topics PF (10 hr)
  - Errata Core plus Error Annex PF (1.5)
  - Runtime Services JH, EB, JH, BL (2)
  - BA Errata PD, EB, JP, BRL (30m)
  - Network Annex informal Ballot (Alexey) (1.0)
  - Security Annex Draft (DG) (1.5)
  - FACE Annex Ballot (TS) (1.5)
  - Total 19 hours
  - Tutorial Workshop (All day Thursday)

# AADL Tool Integrations – All - [Update Wiki](#)

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

Jose Mesquer - AADL/MAUDE –

Jean Pierre Talpin/Brian Larson - AADL/Polychrony/Signal with BLESS

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 into OSATE

Brian Larson - AADL/BLESS

Etienne Borde - AADL/Behavior Annex, RAMSES

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/FMI ... 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...

ESA – TASTE, COMPASS (upgraded to use standard AADL)

D-MILS – Security and Safety with compositional verification and system synthesis

WWT – Editor and analysis tools

SCADE – has added AADL, [released commercial version Jan 2018](#)

Dassault Systems – [Translator to AADL, Integration with AADL Inspector](#)

# Actions

Action	Date	Lead	OK
Denis to provide Peter with default semantics for ports in ARINC653, related to a more abstract port	1/18	DB	
Jerome to send Peter FMI description language for continuous and discrete ports when available mid 2018.	1/18	JH	
Network Annex using Data volume but should we use data rate unit type? Peter will supply recommendation to Alexey	1/18	PF	
Alexey to email Steve Vestal to get needed definition for Max_Supported_VLS.	1/18	AK	
Alexey to contact Eric Jenn to see if he needs TTE example but we have the properties defined now.	1/18	AK	
V3 Configuration Parameter Match and Replace, Denis to provide example patterns to Peter	1/18	DB	
AADL Core Errata – Peter will contact Steve Vestal to understand purpose of priority extension request.	1/18	PF	

# Actions

Action	Date	Lead	OK
AADL Code Gen Annex questions – RTS to make type safe, report error types, send output detection, periodic dispatch management. Jerome will coordinate with Mike, Etienne, Brian	1/18	JH	
Jerome to discuss new concepts in ARINC 653 related to Binding	5/18	JH	
Etienne to discuss ARINC 653 related to managing errors/recovery points	5/18	EB	
	11/18		
	11/18		
	11/18		
	11/18		

# Actions

Action	Date	Lead	OK
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		

# Actions

Action	Date	Lead	OK
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		
	11/18		

# BACKUP

# Actions

Action	Date	Lead	OK
Demonstrate FMI/AADL for Sept 25 meeting	1/17	JH	
Trademarks – Bruce will ask Dorothy (author just asks perm)	1/17	BL	x
Exploring Binding software flows to hardware flows, trees of flows	1/17	Alexey	
Example to GITHUB for reverse interfaces	1/17	PF	
Send formula for expressing Arrays to Peter	1/17	BL	x
Send out slides on arrays, consider Brendan's input	1/17	PF	
Unified Type System examples	1/17	LW	



# Actions

Action	Date	Lead	OK
Consider AltaRica feedback to improve EMV2	1/17	PF, LW	x
Send Brian the BNF for transistions, the encoding in SIGNAL	1/17	JP	
Recommendation – Before formalization, lets look at syntax, semantics for runtime services, then go to formalization annotations as a separate annex., Lead effort.	1/17	EB	x
Provide updates and errata for ARINC Annex	1/17	Alexey, Denis	x
Lay out scope of the security annex	1/17	DG	x
Schedule time to discuss tree flows as part of V3	6/17	BAL	x
Organize telecon with Bren and Peter to develop ideas for proposal on arrays	6/17	BRL	

# Actions

Action	Date	Lead	OK
Supply suggested improvements on “refines to” to Peter	6/17	SV	
Set up telecon to discuss with Alexey, Peter, Brendan, Steve the blended use of the error modeling and networking annexes	6/17	PF	
Set up a telecon on the runtime services with Jerome, John, Brian, and Etienne	6/17	BRL	x
Send an example/questions on runtime context variable for accessing ports to Jerome	6/17	EB	
Present upgrades needed to 653 Annex, like additional properties	6/17	SV	x
	9/17		
	9/17		

# Actions

Action	Date	Lead	OK
	9/17		
	9/17		
	9/17		
	9/17		
	9/17		
	9/17		
	9/17		

# Actions

Action	Date	Lead	OK
	5/18		
	5/18		
	5/18		
	5/18		
	5/18		
	5/18		
	5/18		