SAE Architecture Analysis and Design Language

AS-2C AADL Subcommittee Meeting

Feb 11-14, 2019

Huntsville, AL, USA

AADL

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 11-14 2019 Huntsville, Al. Special Demo Day (Tool Expo) on the 14th.

Spring 2019 –June 24-27 Paris

    Invitation from Patrick Farail do a special track for European Conference on Software Architecture, https://ecsa2019.univ-lille.fr/tracks/industrial-program

    Sept 9-13 in Paris, University de Lille, should we consider Paris for Fall, make June in Minneapolis?

Fall 2019 - Oct 21-24 US - Scottsdale, AZ, Aviation Systems Division, at Hilton, rooms 199/night

Winter 2020 – Jan 2020 Toulouse with ERTS.

Spring 2020 – May Minneapolis ? Or Pittsburgh?

AADL

13th European Conference on Software Architecture (ECSA)

The European Conference on Software Architecture (ECSA) is the premier European software architecture conference, providing researchers, practitioners and educators with a platform to present and discuss the most recent, innovative and significant findings and experiences in the field of software architecture research and practice. The 13th European Conference on Software Architecture (ECSA 2019) will be held on 9-13 September 2019 in Paris, France at FIAP Jean Monnet.

- Architectural design, analysis and evaluation
- Architecture description languages and meta-models
- Architecture verification and validation
- Management of architectural knowledge, decisions, and rationale
- Architecture-based synthesis, code generation
- Architectures for cyber-physical systems and IoT
- Software architecture and continuous integration, continuous development and DevOps
- Architecture-centric model driven engineering
- Component-based models and deployment, middleware
- Software tools and environments for architecture-centric software engineering
- Empirical studies, systematic literature reviews and mapping studies in software architecture.
- Workshop proposal **March 7, 2019**   Industrial Presentations **May 31, 2019**

AADL

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.
  - SAE 5 year review, Need to select a status,
    https://www.sae.org/standards/development/definitions/
  - Data Annex has not been updated, 653 and Behavior have. To be revised after V3

- 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**

AADL

SAE Document Status

- **Standards Status Definitions**
- *(Effective December 2010)*
- **Issued**
- First time a technical report is published. Subject to 5-year review.
- **Revised**
- An active technical report has been updated and re-published. Subject to 5 year review.
- **Reaffirmed**
- Technical report which has been reviewed by the technical committee and determined to be current with no need for immediate revision. Subject to 5 year review.
- **Stabilized**
- A technical report that has been 'frozen' at the last active revision level. 5 year review is not required. (ANSI nationally adopted standards subject to 10 year review.)
- **Canceled**
- If published prior to December 31, 2010 defined as: a technical report that is no longer actively being used. A cancelled technical report may be superseded by another technical report. A cancelled action requires Committee and Council level ballot.
- If published after January 1, 2011 defined as: a technical report that is deemed 'not fit for use' due to technical reasons or when its technical requirements are totally superseded by another document. 5 year review is not required.

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.
- FACE Annex AS5506/4 - Discuss ballot.
- Network Annex near ready 5 – Ready to start informal ballot for June 2019?
- Security next – 6? Informal Oct 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. Spring 2020 whole doc: potentially in sections: ADL, Property/type system, thread etc. semantic & RT system
- 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)
- 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

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. LAMP possible?, then discuss June.

- 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 – (90%)(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 (60%)– 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 written by Tyler Smith, finish ballot by Feb 23.

- 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.

AADL

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), Huntsville (Tool Expo), ***So many possible, may need workshop.***

Potential for future meetings:

- Ellidiss AADL Inspector LAMP

- FACE, SCADE Integration w AADL ANSYS

- Adventium FASTAR or TradeSpace or MILS tools

- MASIW

- TASTE

- Next Tools workshop? Who would organize? (94 acceptances for Tool Expo). ESAC?

AADL

International Joint Research

Suggestions:

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

AADL

Planning for June 2019

- Possible User ½ Day
  - Trade-Space Adventium (30min)
  - Space Robotics (Jerome)
  - …
  - …

  - Total 1.0 hours

Standardization

- News (30m)
- Next Meeting Planning and action items (30m)
- **AADL V3.0** topics PF (11 hr)
- Errata Core plus Error Annex PF (1)
- **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)

- Total 19 hours

- Tutorial Workshop (LAMP or FASTAR?) (3.0)

AADL

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

AADL

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	x
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	x

AADL

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	x
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	
Confirm June 10-13 for next meeting	11/18	DB	
Generate UUID from AADL to FACE in Annex	11/18	TS	x
Next Meeting discuss V3 flows	11/18	PF	
Next meeting Set up day for tool demonstrations	11/18	BL	x

Actions

Action	Date	Lead	OK
Do we need to use BA in Security Annex for state machine for control of Key	11/18	DG	
Produce draft document for Security Annex	11/18	DG	
Session on SysML/AADL Guidance for next meeting	11/18	BL, TL, JH	
Develop concept for safety layer on Network, coordinate with Mirko	11/18	BH	
Simplifications for OSATE that would allow it to run stand alone.	11/18	DB, LW	
ANT tasks for the workflow language of ParisTech	11/18	DB, TS	
Need Errata for Code Generation Annex, it's out of date, example subprogram parameters rather than input port	11/18	JH	

AADL