AADL/ACVIP User Day 2022

ACVIP in Practice at Sikorsky / Lockheed Martin

Scot Wrocklage & Alek Taraskewich

Carnegie Mellon University
Software Engineering Institute

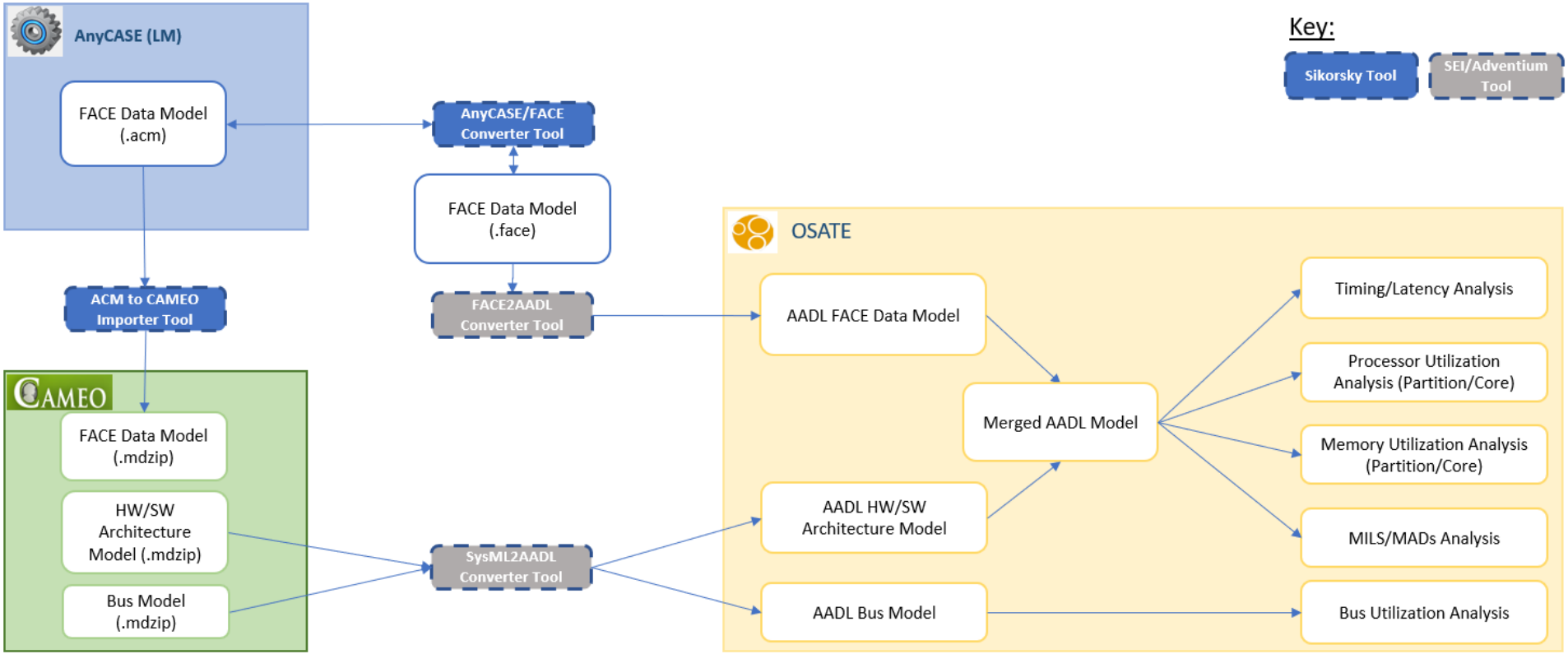
This work was done under U.S. Army DEVCOM AvMC Contract # W911W6-19-2-0003.

Public Information Release Authorization (PIRA) SIK202205021

Agenda

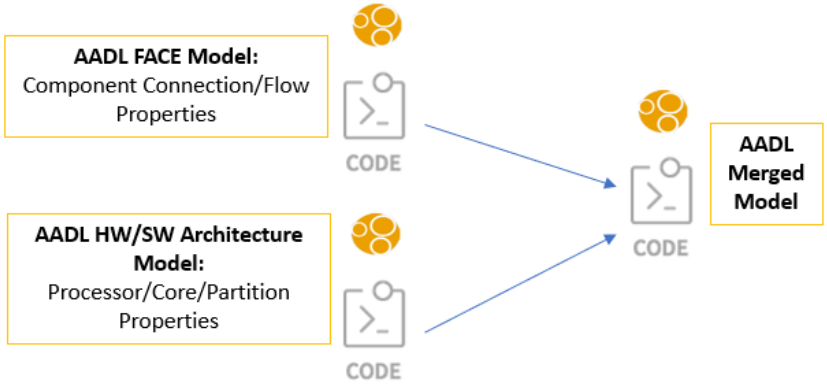
- Sikorsky ACVIP Tooling and Process Visualization
- AADL Translation Tools
- Subsystem Processor/Memory Utilization Analysis
- Subsystem Latency Analysis
- Subsystem MILS/MADS Security Analysis
- System Network Utilization Analysis
- CAMET CVIT and DSI Pipeline

ACVIP Tooling and Process Visualization



AADL Translation Tools

- SysML AADL Bridge* and FACE Data Model to AADL Translator** tools allow for reusability in the development process.
  - Capability to generate AADL models from SysML/FACE models.
  - Allows for maintaining single source of truth within SysML model.
  - Prevents need to replicate data that exists in the FACE model.

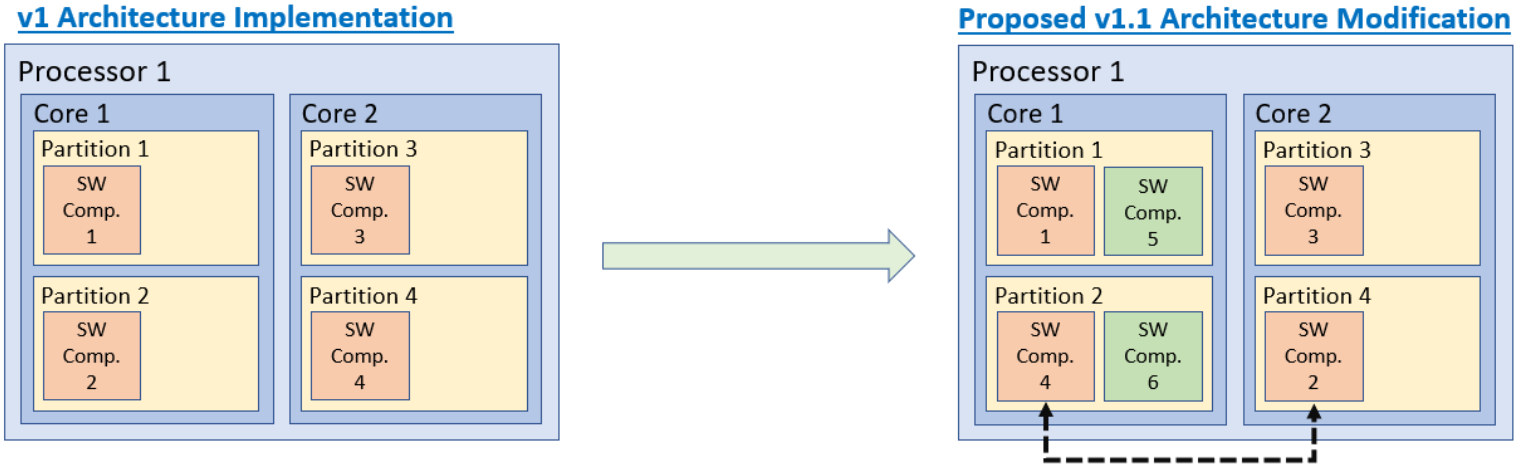


- Sikorsky's current process of using both translation tools, generates two separate AADL models that represent different layers of the system.
  - Sikorsky manually merges both AADL models to complete the system.
  - Exploring potential automated solution for merging models.

*SysML AADL Bridge tool is provided by Adventium Labs.
**FACE Data Model to AADL Translator tool is provided by CMU SEI.

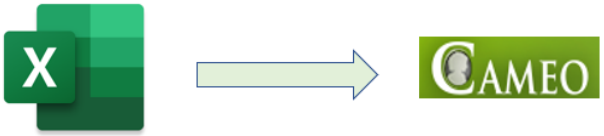
Subsystem Processor/Memory Utilization Analysis

- AADL model that represents architecture centric hardware and software resource supplies/demands.
- Sikorsky uses this model to virtually test design tradeoffs within the subsystem.
  - Software components can be moved within the architecture and the analysis will determine if the hardware supply can meet a change in demand.
  - Sikorsky sees time/cost savings as design changes do not require source code modification or target execution to determine feasibility.
- HW/SW Architecture model hosted in CAMEO allows for a visualization of the system design.



Subsystem Processor/Memory Utilization Analysis

- The OSATE AADL environment allows for either OSATE or 3rd party tools (Adventium Labs' FASTAR Utilization Analysis) to be used for executing analysis and viewing reports.
- The analysis report represents the system at a discrete time for metrics reporting.
  - Replaces manually calculated methods and eliminates the need to manage the same data in a different tool.



Subsystem Processor/Memory Utilization Analysis

- The Adventium Labs' CAMET tool suite includes the ability to customize analysis reports using the Report Generator tool.
  - Report data formatting can be modified/enhanced.
  - Report data can be post processed and more advanced metrics can be computed.

Default Template

Utilization Analysis

Generated: May 17, 2022 9:51:17 AM

Mode: system.no-mode

Resource: Processor.Core_0

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	1500				

Resource: Processor.Core_0.Partition1

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	1000	995	1	1	1.01
Process1	1000	995	1	1	1.01

Resource: Processor.Core_0.Partition2

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	500	500	1	1	1
Process2	500	500	1	1	1

Custom Template

Utilization Analysis

Generated: May 17, 2022 9:48:58 AM

Resource: Processor.Core_0

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	1500	1,495.004	99.667%		

Resource: Processor.Core_0.Partition1

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	1000	995	99.5%	1	1.005
Process1	1000	995	99.5%	1	1.005

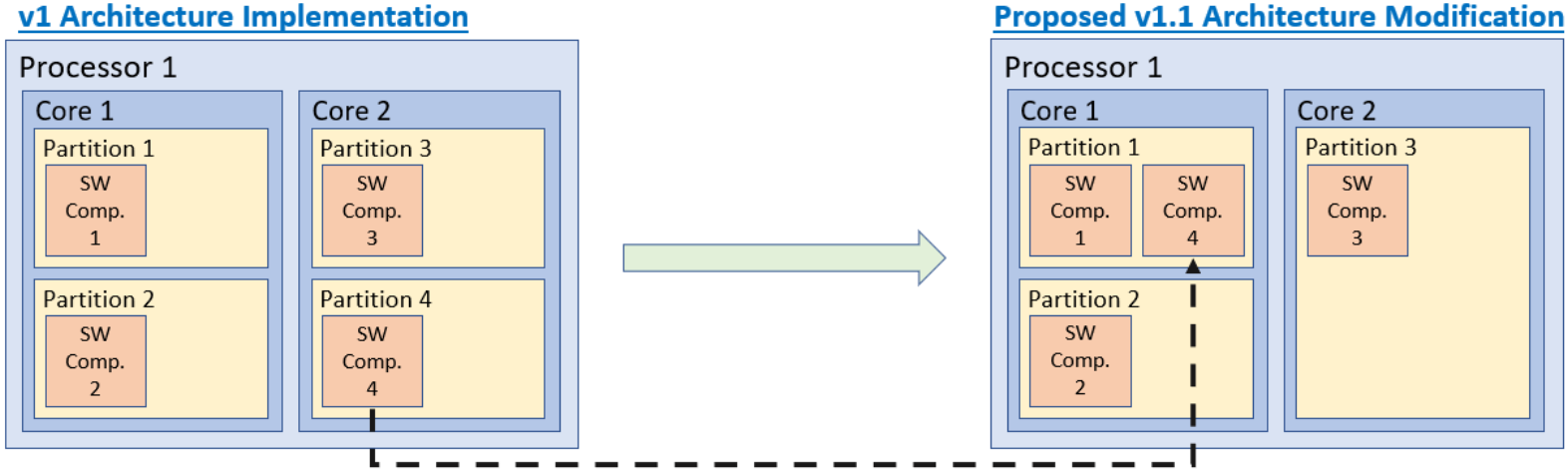
Resource: Processor.Core_0.Partition2

Demand	MIPS Supply	MIPS Demand	MIPS Util	MIPS U Limit	MIPS Margin
All	500	500	100%	1	1
Process2	500	500	100%	1	1

ACVIP in Practice at Sikorsky / Lockheed Martin

Subsystem Latency Analysis

- Captures end-to-end timing or latency metrics for two or more software components within a VxWorks RTOS subsystem.
  - "AADL Annex for FACE"*, defines that each UoP (Software Component) is modeled in AADL as a thread group.
  - "SysML AADL Profile and Modeling Guidelines"*, state that subprogram parameters and call sequences are not currently supported.
- Subsystem latency will be utilized for time sensitive domains where strict timing must be enforced.
  - Display of primary flight data.
  - Sensor data to mission functions.
- Allows for virtual integration to ensure that any architecture modification with latency impact, can be analyzed prior to code modification.



*Documents provided by Adventium Labs.

Subsystem MILS/MADS Security Analysis

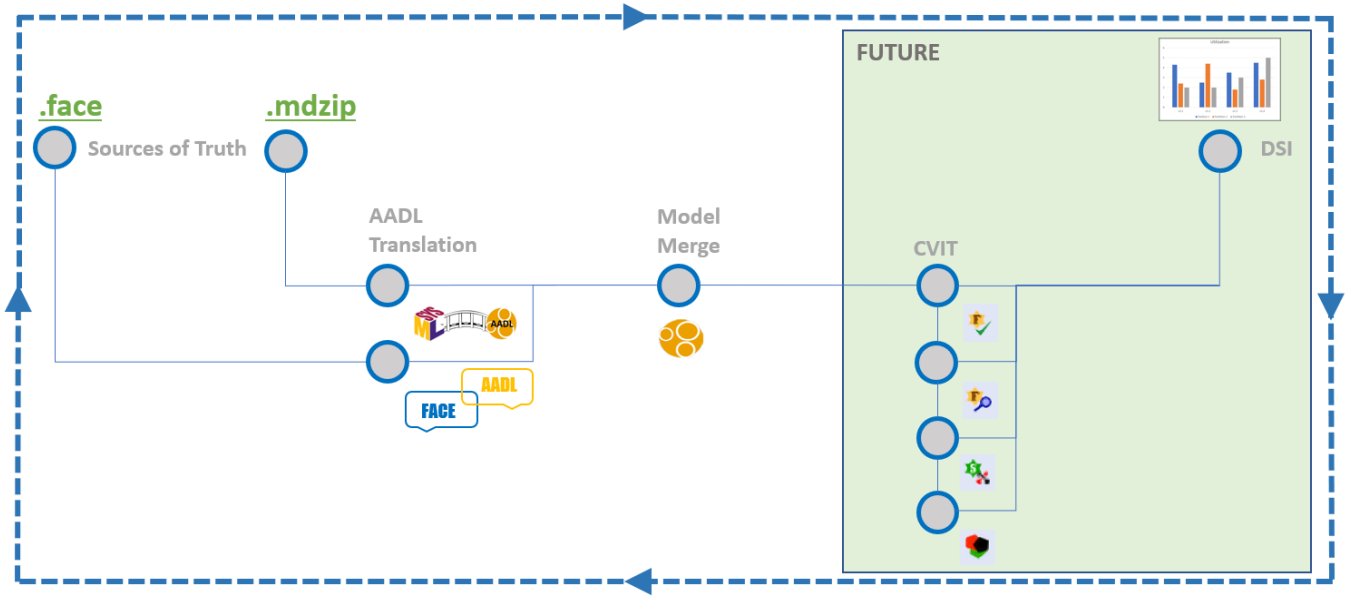
- Multiple Independent Levels of Security (MILS) analysis will determine if any components within the HW/SW architecture that are directly connected, operate at the same security level and that separation is implemented with an appropriate security measure.
  - MILS analysis can be evaluated against evolving cyber requirements as a means of model based confirmation of the system's cyber assurance design.
- Multiple Analyses for Domain Separation (MADS) analysis allows for domains and boundaries for components to be defined in the HW/SW architecture model and ensures that separate domains do not share components.
  - Evaluating potential for MADS analysis to assure lower design assurance level (DAL) data does not cross into higher DAL functions.

System Network Utilization Analysis

- Captures ethernet bus network utilization between higher level end systems.
- Ensures that that bandwidth supplies of the network meet the demands of the message traffic.
- The bandwidth utilization model can be used to test virtual integration of the network and ensure that any message/interface modification meets the bandwidth supply, prior to code or network configuration changes and target deployment.
- Sikorsky is evaluating a model solution to analyze a deterministic, fixed message scheduling system.

CAMET CVIT and DSI Pipeline

- Sikorsky plans to automate the analysis execution process using Adventium Labs' Continuous Virtual Integration Toolkit (CVIT) to expand upon existing software factory infrastructure.
- Sikorsky plans to use the Adventium Labs' Design Space Investigator (DSI) tool suite to track model changes and analysis outputs over time.



Presenters

Scot Wrocklage

Associate Fellow and Software Architect

scot.m.wrocklage@lmco.com

1-203-383-8212

Alek Taraskewich

Senior Software Engineer

alek.e.taraskewich@lmco.com

1-203-385-1353