Collaboration Conversation
Scalable Assurance of Safety-Critical Systems

Sholom Cohen, Jerome Hugues, Sam Procter
Moderated by SuZ Miller
Create the best design that holds up over time as the system evolves. + Test the design without having to write any code. = Build a single model to assess hardware and embedded software before the system is built.

**SAE AADL / ACVIP**
Standardized language and process for the engineering safety-critical systems.

**OSATE**
Open Source AADL toolset for performing verification and validation (V&V).

**DoD Transitioning**
Maturity increased through pilot projects and trainings.
AADL Standard Suite (AS-5506 series)

Core AADL language standard [v1 2004, v2 2012, ... **v2.3 2022Q1**]
- focused on *embedded system architecture: modeling, analysis, and generation*
- strongly typed language with well-defined semantics, rich property sets for capturing performance, safety, and security
- annexes: safety, avionics (ARINC653, FACE), behavior, code generation

AADLv2.3: minor revision to address new architecture needs
- patterns for multicore systems, updates to ARINC653
- clarification of semantics of threads (core), operation on errors (EMV2)
SAFIR: Assuring AI/Autonomous Cyber-Physical Systems

An autonomous car is both

- A car with CPUs inside for navigation, engine control, etc.
- A “car and its environment” inside CPUs to make informed decision for driving, braking, etc.

How to assess system safety?
What is the contribution of architecture to AI safety?
This **autonomous CPS** is **safe** because

- It does **reqs**; it is implemented by **arch+code**.
- V&V **activities** demonstrate strict conformance.
- It is operated **safely** and **hazards or threats** are monitored and mitigated by **FDIR**.

SAFIR is building a comprehensive approach to support both systems engineering and safety assessment processes *through*

- tool-support, architectural patterns at both model and runtime levels, new analysis capabilities, and
- an argument the above are self-consistent
Model-Based Systems Engineering & Safety

- **Core Idea:** Embed information where it’s relevant
- Language features useful to variety of stakeholders
  - Used by tooling to automate common tasks / generate reports
Architecture Centric Virtual Integration Process (ACVIP)

Research Objectives

• Integrate ACVIP into MBSE across the lifecycle—emphasis on addressing risk to program goals (cost, schedule, performance).

• Emphasize modeling with analysis as the goal not “Architecture as Artwork” (Phil Zimmerman).

• Move modeling and analysis to the left.

<table>
<thead>
<tr>
<th>Application of Modeling and Analysis</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make tradeoffs</td>
<td>Reuse of proven modeling and analysis results</td>
</tr>
<tr>
<td>Refine specifications</td>
<td>Scenario based acquisition support for specification refinement</td>
</tr>
<tr>
<td>Early discovery of defects</td>
<td>“Ubiquitous testing”</td>
</tr>
</tbody>
</table>
Effort Invested vs. Effort Saved During S&T

Apply research to transition from Science & Technology (S&T) to operation.

- Increased early involvement in modeling
- Total development effort reduced by 30%
The Panel

SuZ Miller
Moderator, Principal Researcher

Sholom Cohen
Principal Engineer

Dr. Jérôme Hugues
Principal Investigator, Senior Architecture Researcher

Dr. Sam Procter
Senior Architecture Researcher
Research Team

Dr. Jérôme Hugues
Principal Investigator, Senior Architecture Researcher

Dr. David Gluch
Software Architecture Researcher

Dr. Aaron Greenhouse
Senior Architecture Researcher

Keaton Hanna
Assistant Software Engineer

John Hudak
MTS, Principal Engineer

Dr. Sam Procter
Senior Architecture Researcher

Dr. Chuck Weinstock
Principal Researcher

Lutz Wrage
Senior Member of the Technical Staff