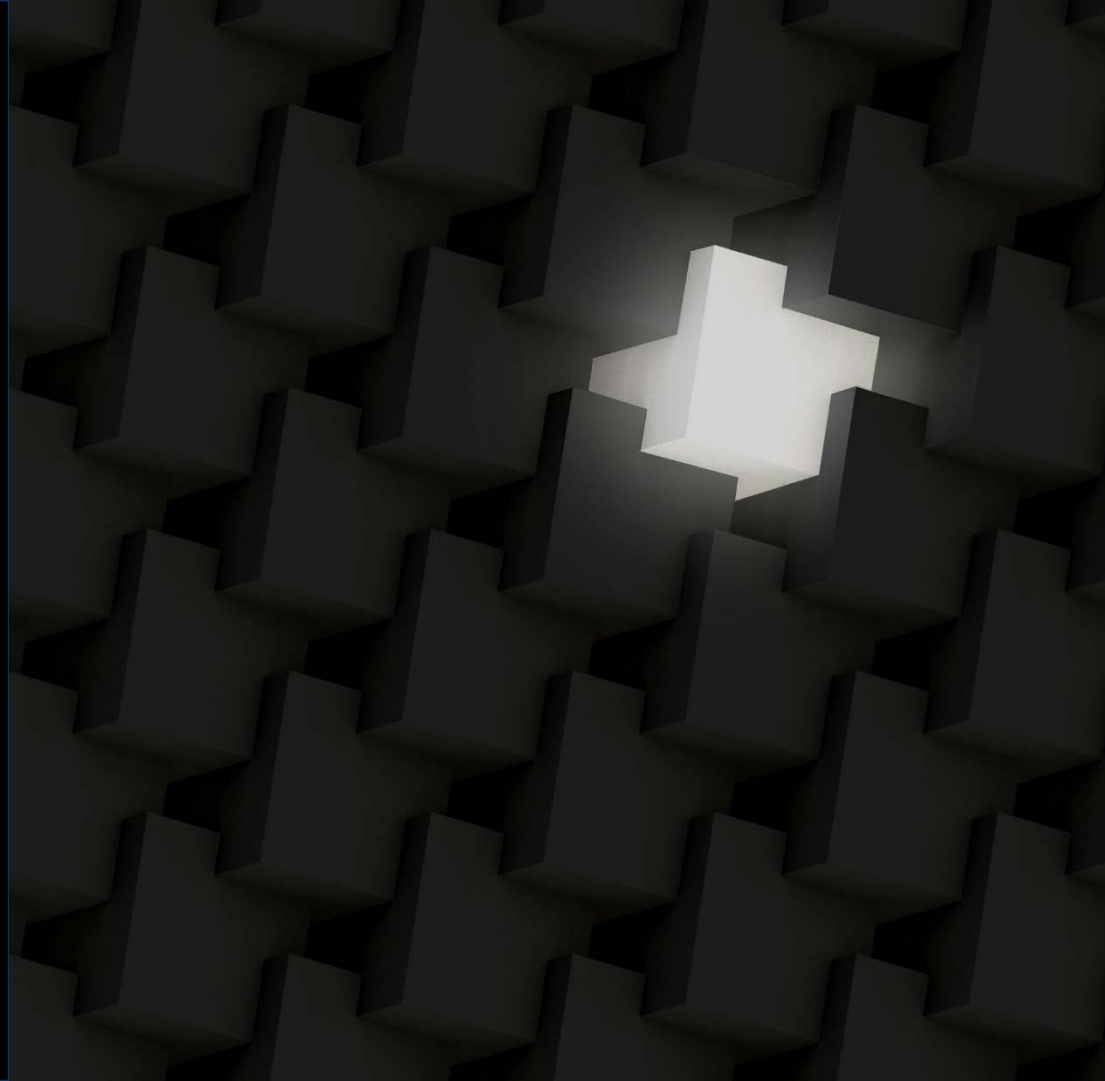


Carnegie Mellon University
Software Engineering Institute

RESEARCH REVIEW 2020

Model-Based Engineering with
AADL: Transitioning Research to
Practice

Sam Procter



Document Markings

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0814

Outline

The Problem: Safety-Critical Embedded Software Systems

- Part of the Solution: AADL Framework

How AADL Helps Solve Problems

- Our Current Project
- Zooming Out: Safety Work Done by the MBE Team
- Zooming Out, Again: A Holistic View of Research Using AADL

DoD Impacts: Army AADL Success Story

- Not Just DoD: How AADL Supports Transition

Alignment with Digital Engineering Strategy

RESEARCH REVIEW 2020

Model-Based Engineering with AADL: Transitioning
Research to Practice

The Problem: Safety-Critical Embedded Software Systems

The Safety-Critical Embedded Software System Challenge

Problem:

- Software increasingly dominates safety and mission-critical system development
- Issues discovered long after they are created

Goal:

Early discovery of system-level issues through virtual integration and incremental analytical assurance

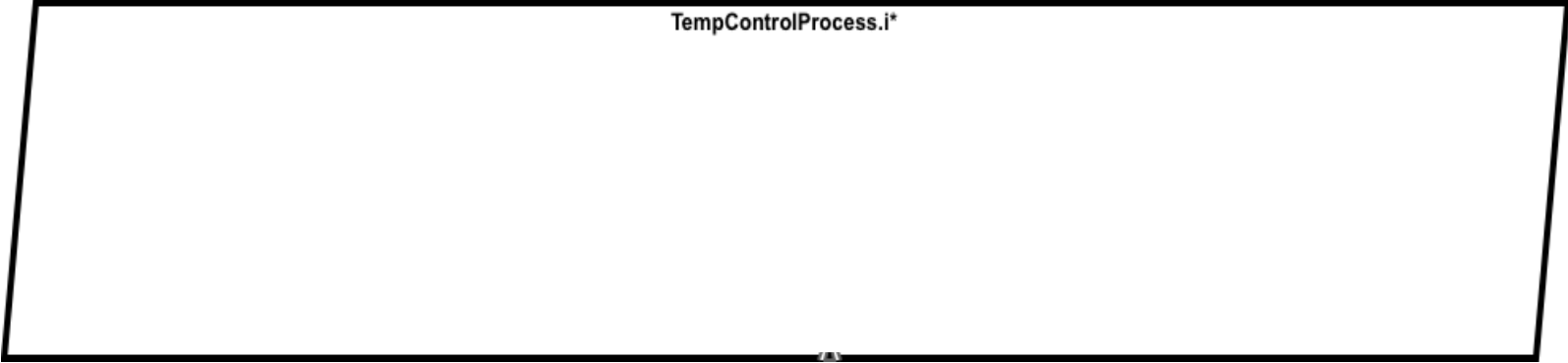
Solution:

- **Language** standardized via SAE International & matured into practice through pilot projects & industry initiatives
- **Tooling** available under open source license continually enhances analysis, verification, and generation capabilities
- Direct alignment with DoD Digital Engineering Strategy



A critical task: Reducing safety and security risks through early analytical assurance

AADL Overview



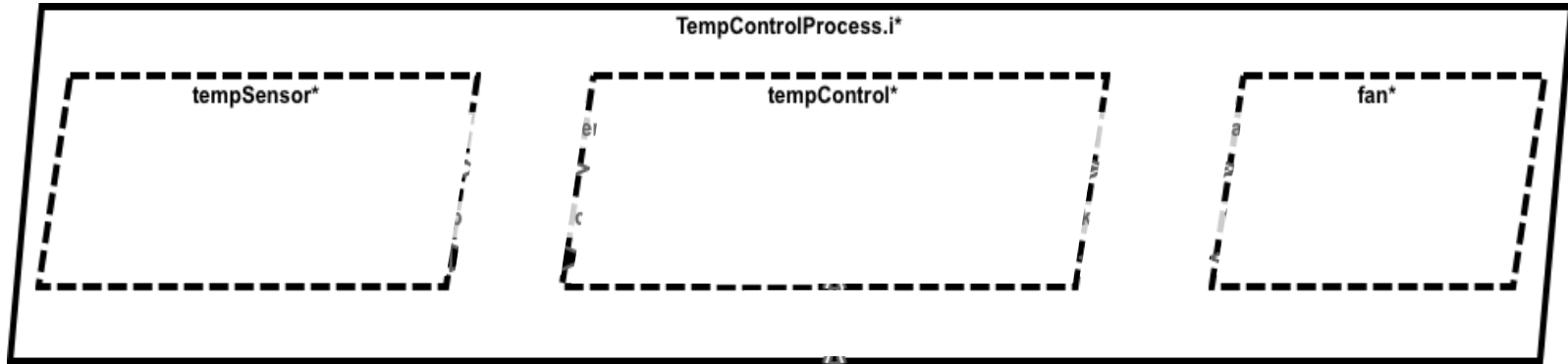
TempControlProcess.i*

Like a lot of models that engineers draw every day on their whiteboards, AADL consists of boxes and lines

The difference between AADL and a whiteboard is that AADL has precise *semantics*

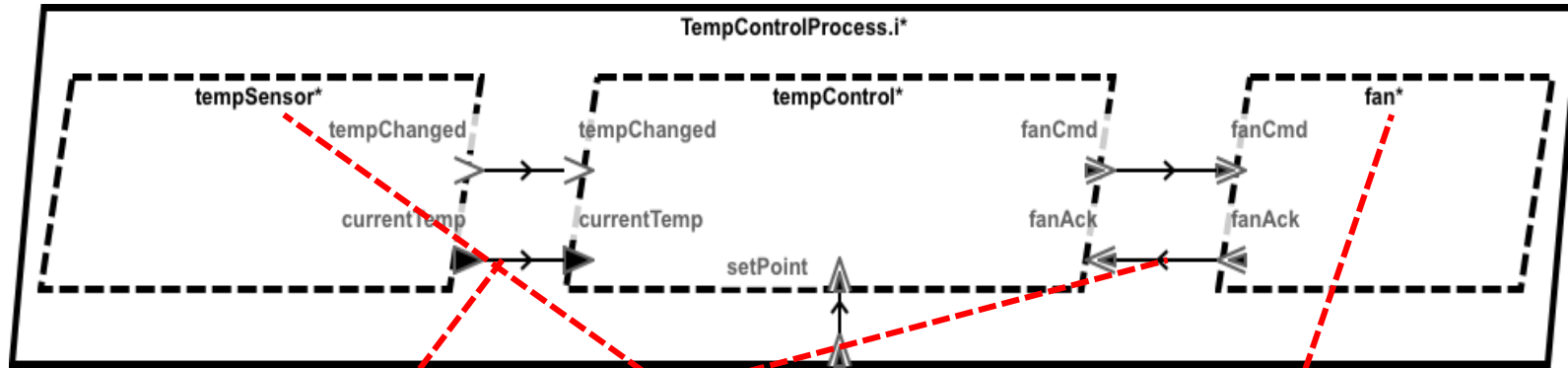
This box represents a computer process – a protected region of memory and a space where we can allocate individual threads

AADL Overview



Those threads are also boxes – but they have very precise meanings.

AADL Overview



We can connect the threads together using lines to represent different types of intra-process communication

We add more semantics via *properties* – they are useful for both system analyses and to guide code generation

This box shows a periodic thread – it is dispatched regularly according to some clock

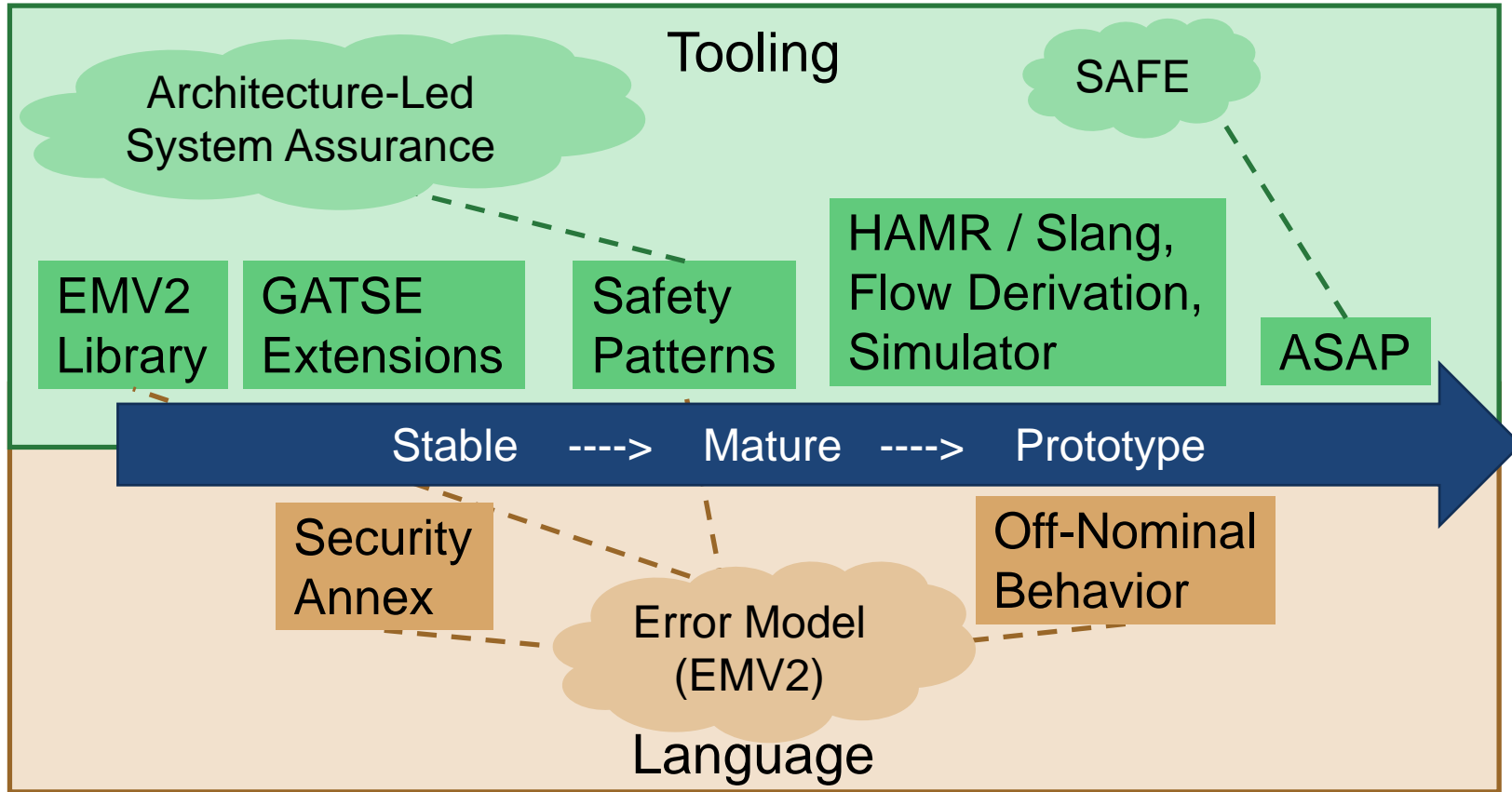
And this thread is sporadic – it is dispatched whenever a message arrives at a specified port

RESEARCH REVIEW 2020

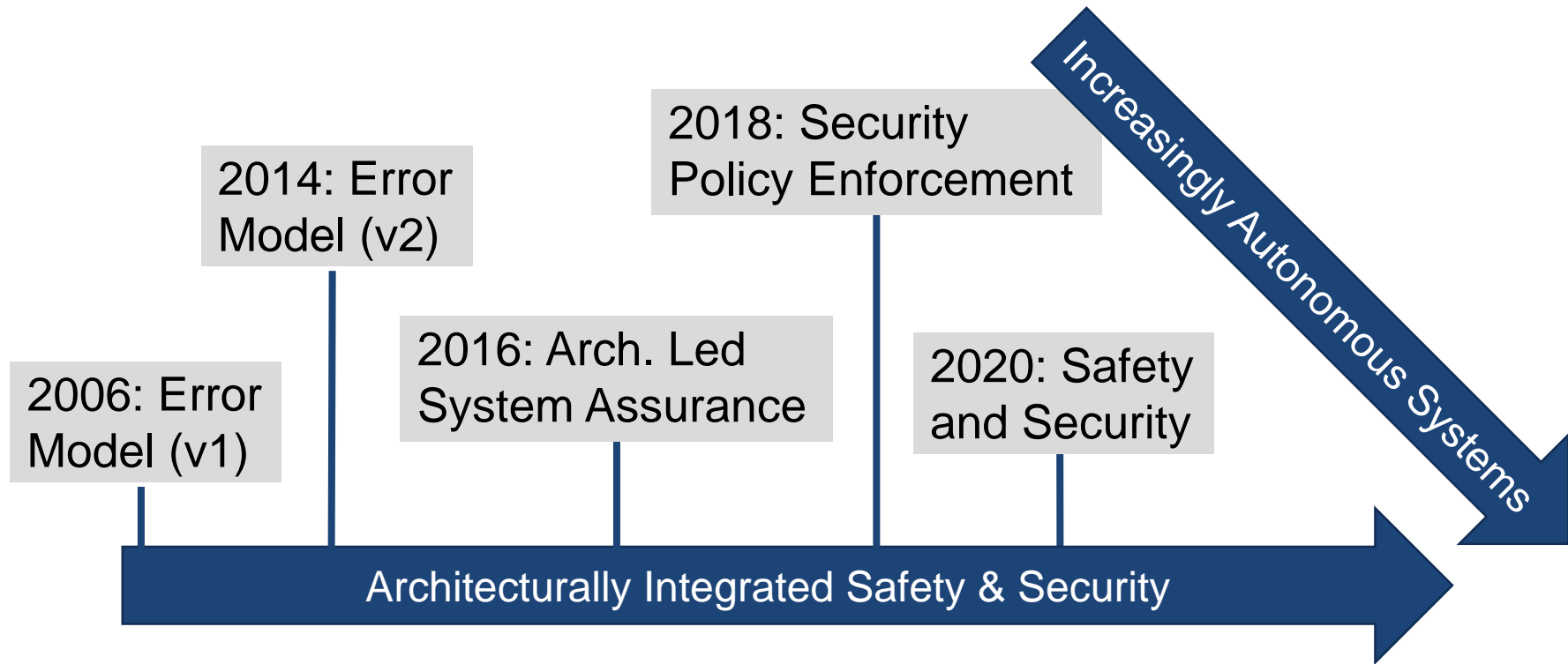
Model-Based Engineering with AADL: Transitioning
Research to Practice

How AADL Helps Solve Problems

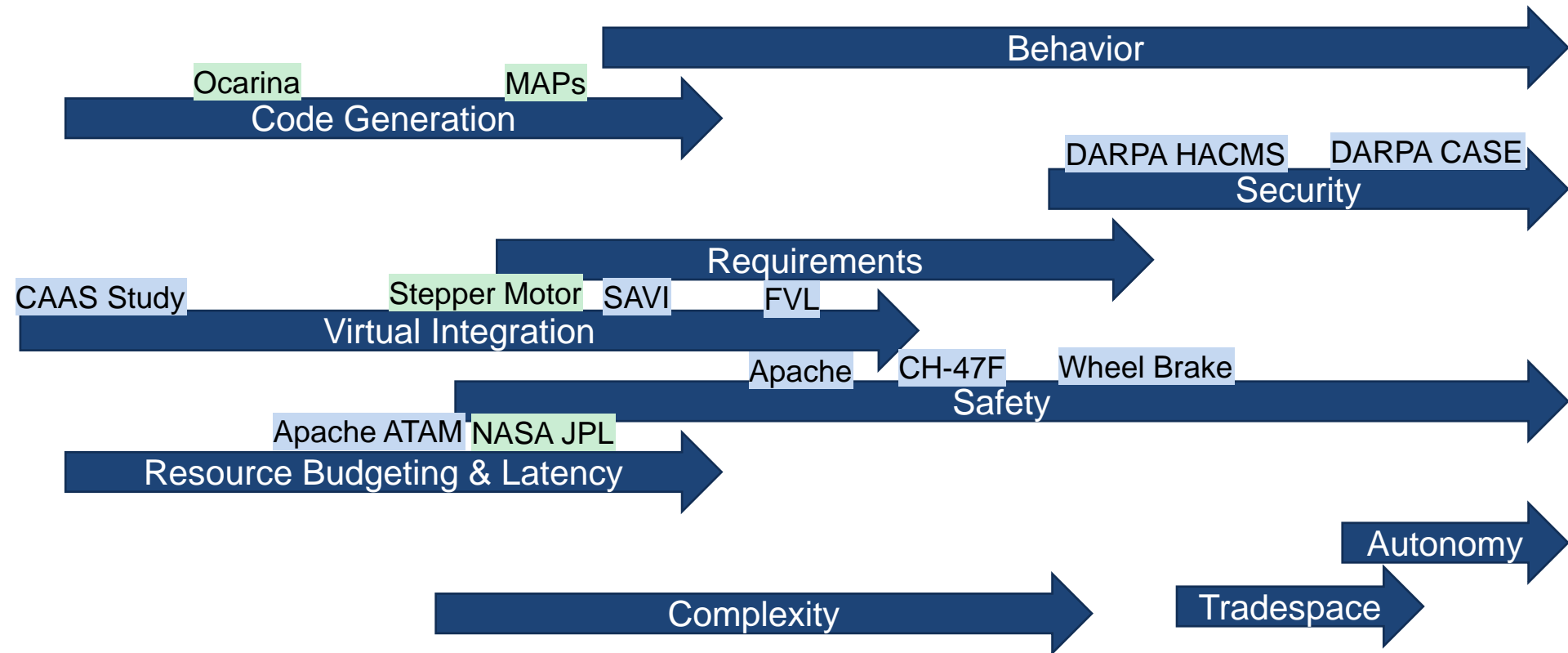
Integrated Safety and Security Engineering (ISSE)



AADL and Safety: The Work of the Model-Based Engineering Team



A Holistic View of Lines of Research Enabled by AADL



RESEARCH REVIEW 2020

Model-Based Engineering with AADL: Transitioning
Research to Practice

DoD Impacts: Army AADL Success Story

Helping to Revolutionize Army Aviation

Over many years, the SEI has had an outstanding partnership with the U.S. Army, which is at the vanguard of applying AADL and ACVIP to the Army's future vertical lift challenge.



Benefits of AADL & ACVIP (via Alex Boydston)

- Decreased fielding time by finding problems early
- Early risk reduction by discovering performance issues early
- Increased cybersecurity by using AADL/ACVIP to improve system security
- Decreased development costs and support for MOSA and certification by transforming procurement supporting MBE and ACVIP



Image source: army.mil

Virtual integration of software, hardware, and system supports verification, airworthiness, safety, and cybersecurity certification

Impact

Finding Problems Early (AMRDEC/SEI)

Summary: 6-week virtual integration of health monitoring system on CH47 using AADL

Result: Identified 20 major integration issues early

Benefit: Avoided 12-month delay on 24-month program



CH47 Chinook

High Assurance Cyber Military
Systems (HACMS)



Unmanned
Quadcopter

TARDEC
Autonomous Truck

Improving System Security (DARPA/AFRL)

Summary: AADL applied to unmanned aerial vehicles & autonomous truck

Result: AADL models enforced security policies and were used to auto-build the system

Benefit: Combined with formal methods verification, prevented security intrusion by a red team

Transforming Procurement (Joint Multi-Role)

Summary: Industry/DoD process demonstration

Result: Pre-integration fault identification

Benefit: 10X reduction integration test cost

All image sources: army.mil

Makes complex capabilities possible through Agile analytic and virtual integration of real-time safety- and security-critical cyber-physical embedded systems

How AADL and SEI Research Enable Transition

Research

- SEI
- K-State
- Telecom Paris
- UMinn
- GTRI
- Adventium

“Valley of Death”

DoD & Industry

- Army
- ANSYS¹
- Dassault
- Ellidiss
- Physical Optics Corp
- Innovative Defense Technologies

¹ <https://www.ansys.com/blog/create-models-architecture-analysis-design-language-aadl>

RESEARCH REVIEW 2020

Model-Based Engineering with AADL: Transitioning
Research to Practice

Alignment with Digital Engineering Strategy

Alignment with Digital Engineering Strategy

June 2018 – Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Michael Griffin (former USD(R&E)): “Those implementing the practices must develop the “how” – the implementation steps necessary to apply digital engineering in each enterprise.”

<https://fas.org/man/eprint/digeng-2018.pdf>

Boydston et al.: “ACVIP plays a key role in addressing issues in cyber-physical systems (CPS) and can be a key contributor to the U.S. Department of Defense (DoD) Digital Engineering Strategy.”

Architecture-Centric Virtual Integration Process (ACVIP): A Key Component of the DoD Digital Engineering Strategy



Image source: *DoD Digital Engineering Strategy*, June 2018

For More Information

Contact Us

Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479

Web: www.sei.cmu.edu

Email: info@sei.cmu.edu