

Research Review 2017

# Automated Assurance of Security Policy Enforcement (AASPE)

Principal Investigator: Peter Feiler, SEI Fellow

Presenter: Sam Procter, Architecture Researcher

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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](mailto:permission@sei.cmu.edu).

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

DM17-0788

# Executive Summary

## 1. *Relevance for the DoD warfighter*

**Safety-critical systems are no longer closed but connected, thus exposed to security threats**

## 2. *Relevance to state-of-the-art in software engineering or cybersecurity*

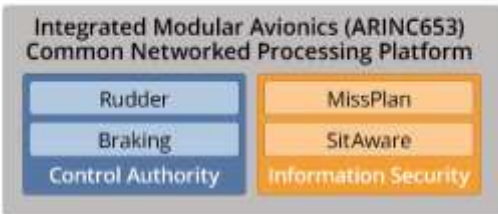
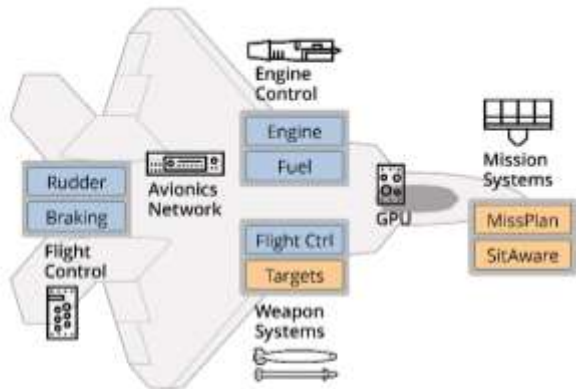
**Avionics industry embraces model-based architecture-centric virtual integration for safety**

## 3. *Expected DoD practice improvements*

**Continuous assurance through automated architecture security analysis to complement code level security analysis**

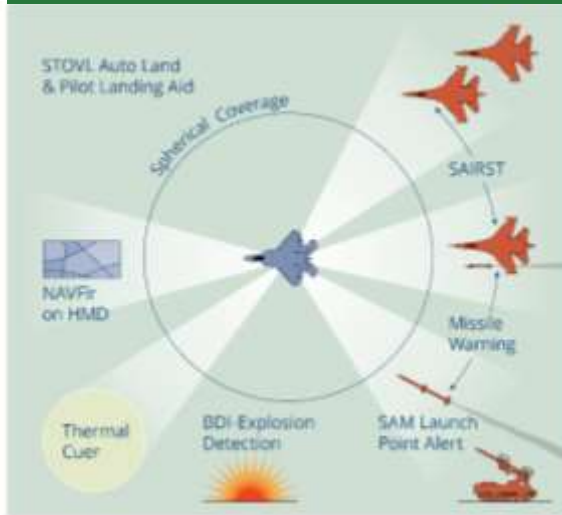
- **Analysis of security policy specifications for vulnerabilities**
- **Analysis of security enforcement runtime architecture for vulnerabilities**
- **Generation of runtime system configurations from verified security models**

# Security Challenges as Safety-Critical Systems Become Connected



**Safety-critical avionics systems use partitioning to achieve fault isolation**

## Good Example: Aviation



**More than secure code and external firewalls**  
Security policy in form of acceptable command and information flows and isolation requirements

**AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX**

## Bad Example: Automotive



**Lack of physical and logical isolation within system leads to costly rework and recalls**

# A Model-Based Analysis and Generation Approach

## Modeling Tool: AADL

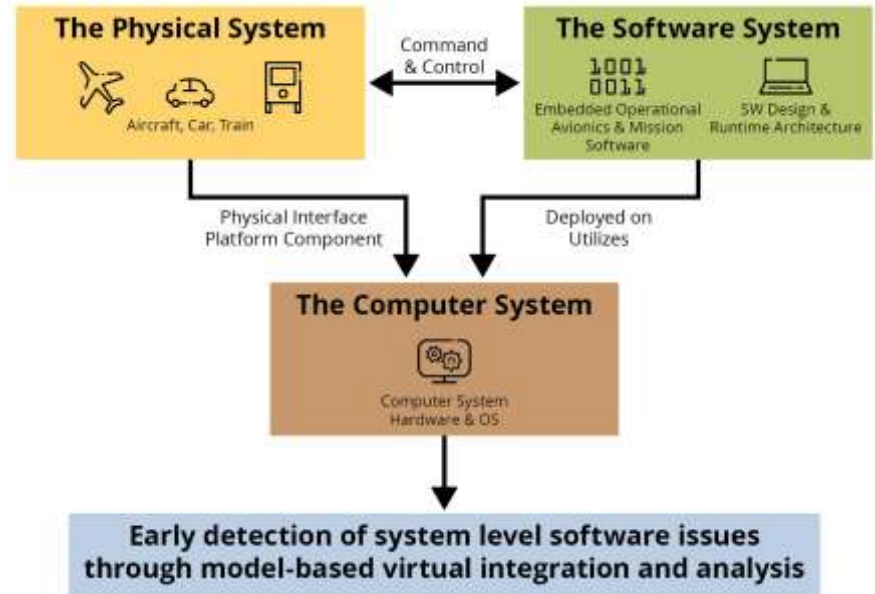
Architecture Analysis & Design Language Widely used standard (SAE International)

- Designed for embedded software systems
- Includes support for timing, performance, safety analysis

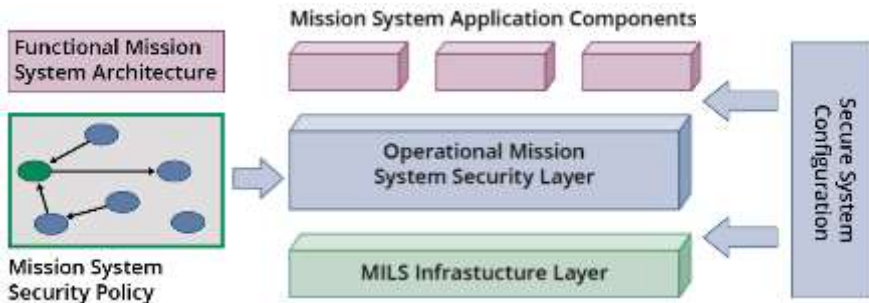
## Extensions:

Model security policy and enforcement

- Security levels/domains
- Trust/verification
- Encryption
- Authentication
- Physical and logical exposure
- Concurrency

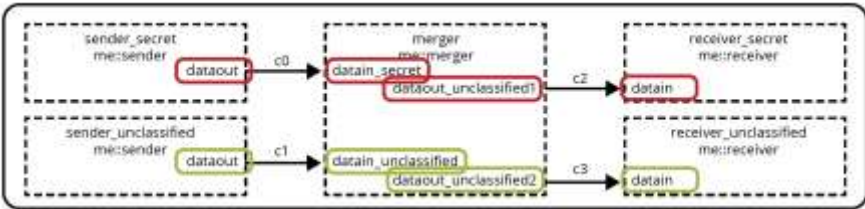
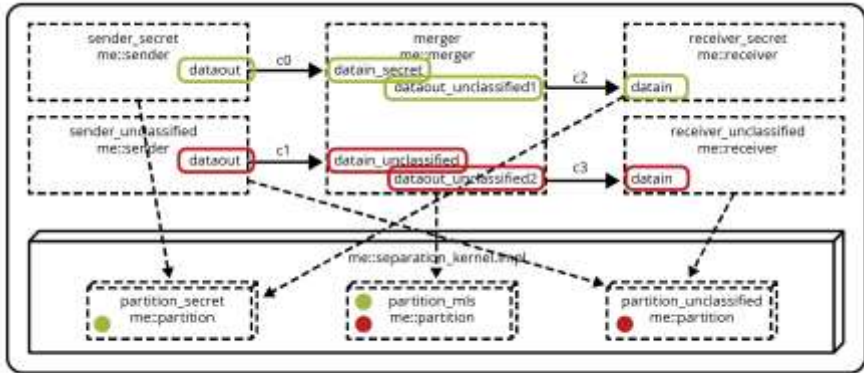


# Vulnerabilities in Security Policies and Their Enforcement



**Security enforcement vulnerabilities: Analyze Deployment Mechanisms**  
 Example: Hi and low-security channels shouldn't coexist on unpartitioned hardware

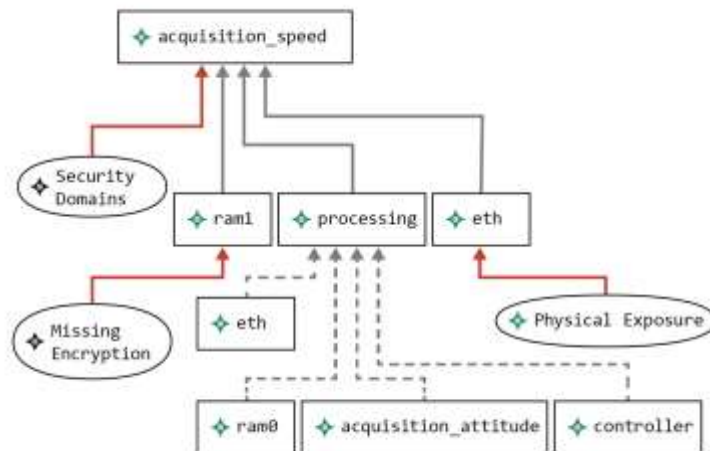
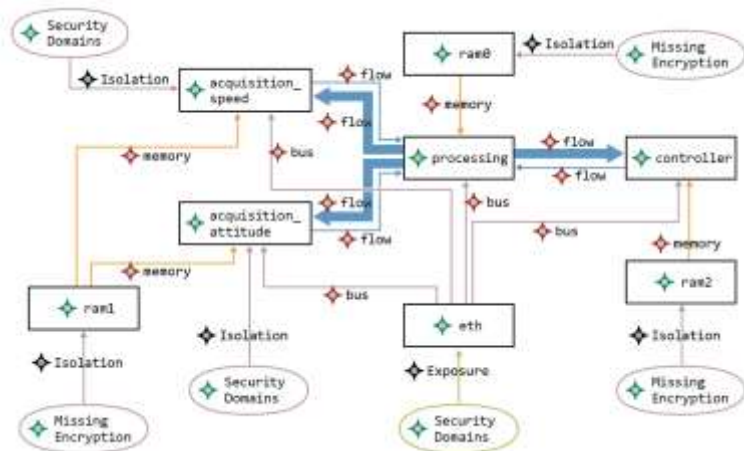
**Security policy vulnerabilities: Analyze Information Flows**  
 Examples: Verify secrets stay secret, and Sensors can't send commands



**Research Connection:**  
 Apply Multiple Independent Levels of Security (MILS) framework (confidentiality) to system security (integrity)

# Security Analysis Techniques and Tools

0. Consistency in security policy specification and enforcement
1. Model-Based Attack Impact Analysis (AIA) tool
2. Model-Based Attack Tree Analysis (ATA) tool
3. Generation of security configuration files
  - Model-based auto-configuration of certified kernel (seL4/CAMkES) security policy

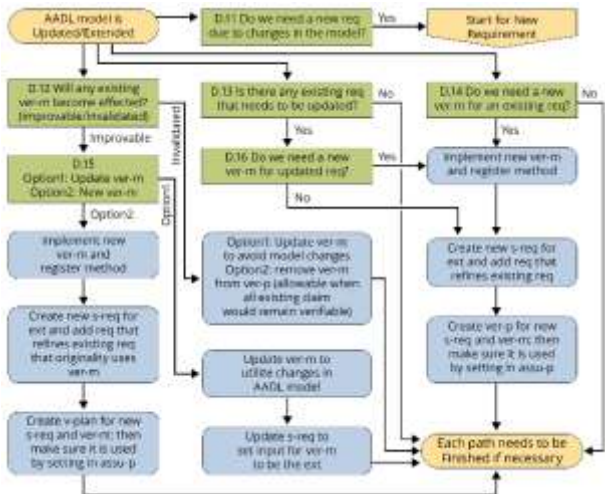




# Using Security Assurance Techniques and Tools

1. Specify security policy as verifiable requirements
2. Formalize verification activities
3. Automate execution of verification plans

## Extension to Architecture-Led Incremental System Assurance (ALISA) workbench



MILS-R0: Components sharing a bus should have the same security level.

MILS-R1: Inter-communicating components should have the same security level.

MILS-R2: Processes with different security levels use isolated memory regions.

MILS-R3: Components associated with identical processing resources share the same security level.

MILS-R4: Threads inside the same process share the same security levels.

CWE-131 Incorrect calculation of buffer size.

CWE-311 Missing encryption of sensitive data.

CWE-805 Buffer Access with Incorrect Length Value.

- 1 System case JeepSecurityCase: (S94 F9 T0 E0 tbd0 ELO T50)
- 2 Model JeepSecurityCase.JeepSecurityPlan(integration.attack)
  - 3 Claim MILS\_R5(integration.attack): MILS\_R5: All non-verifi
  - 4 Claim CWE131(integration.attack): CWE131: incorrect calc
  - 5 Evidence vaCWE131a (203 ms): check connections for c
  - 6 Evidence vaCWE131b (252 ms): Check that timing requ
  - 7 Claim CWE311(integration.attack): CWE311: Missing Encry
  - 8 Claim CWE805(integration.attack): CWE805: Buffer Access
  - 9 Subsystem cellular: (S4 F2 T0 E0 tbd0 ELO T50)
    - 10 Claim MILS\_R0(cellular): MILS\_R0: Components sharing
    - 11 Claim MILS\_R1(cellular): R1: Components with different
    - 12 Claim MILS\_R5(cellular): MILS\_R5: All non-verified com
    - 13 Claim CWE311(cellular): CWE311: Missing Encryption o
    - 14 Claim CWE805(cellular): CWE805: Buffer Access with In
    - 15 Claim MILS\_R6(cellular): R6: All communication that ar
  - 16 Subsystem internet: (S5 F1 T0 E0 tbd0 ELO T50)
    - 17 Claim MILS\_R0(internet): MILS\_R0: Components sharing
    - 18 Claim MILS\_R1(internet): R1: Components with differen
    - 19 Claim MILS\_R5(internet): MILS\_R5: All non-verified com
    - 20 Claim CWE311(internet): CWE311: Missing Encryption c
    - 21 Claim CWE805(internet): CWE805: Buffer Access with Ir
    - 22 Claim MILS\_R6(internet): R6: All communication that ar
  - 23 Subsystem router\_cel: (S3 F0 T0 E0 tbd0 ELO T50)
  - 24 Subsystem car: (S62 F6 T0 E0 tbd0 ELO T50)
  - 25 Subsystem attacker\_cel: (S5 F0 T0 E0 tbd0 ELO T50)
  - 26 Subsystem attacker\_wifi: (S5 F0 T0 E0 tbd0 ELO T50)
  - 27 Subsystem attacker\_internet: (S5 F0 T0 E0 tbd0 ELO T50)



# AASPE Results

Code and Examples on GitHub (<https://github.com/cmu-sei/AASPE>)

- Tools
  - Security policy and enforcement verification on AADL models
  - Graphical attack impact and attack tree analysis tools
  - Generation of attack impact graphs and attack trees from AADL models with security annotations
  - Generation of seL4 configuration files from AADL based specifications
- Example models
  - Automotive: Jeep, Prius
  - Aircraft model
  - Drone case study

Proposal for AADL Security Annex standard

Papers/report on security analysis, security assurance workflow

Proposal for an integrated safety and security engineering approach

# Summary and Future Work

**Where We Started:** DARPA High-Assurance Cyber Military Systems (HACMS) program successfully demonstrated AADL-based verification and generation for reducing vulnerabilities in unmanned drones.

**What We Did:** We demonstrated the feasibility of improving security assurance through architecture modeling and analysis of vulnerabilities in security policy specification and enforcement.

**What's Next for the Community:** Use of SAE International AADL standard offers transition path through the Open Source AADL Tool Environment (OSATE). We will advance the proposed Security Annex to AADL towards approval.

**What's Next for the SEI:** Develop an integrated approach to safety and security engineering approach to mission critical systems funded as new three-year SEI line project.

# Contact Information

## Principal Investigator

Peter Feiler, SEI Fellow

phf@sei.cmu.edu

412.268.7790

## Presenter

Sam Procter

sprocter@sei.cmu.edu