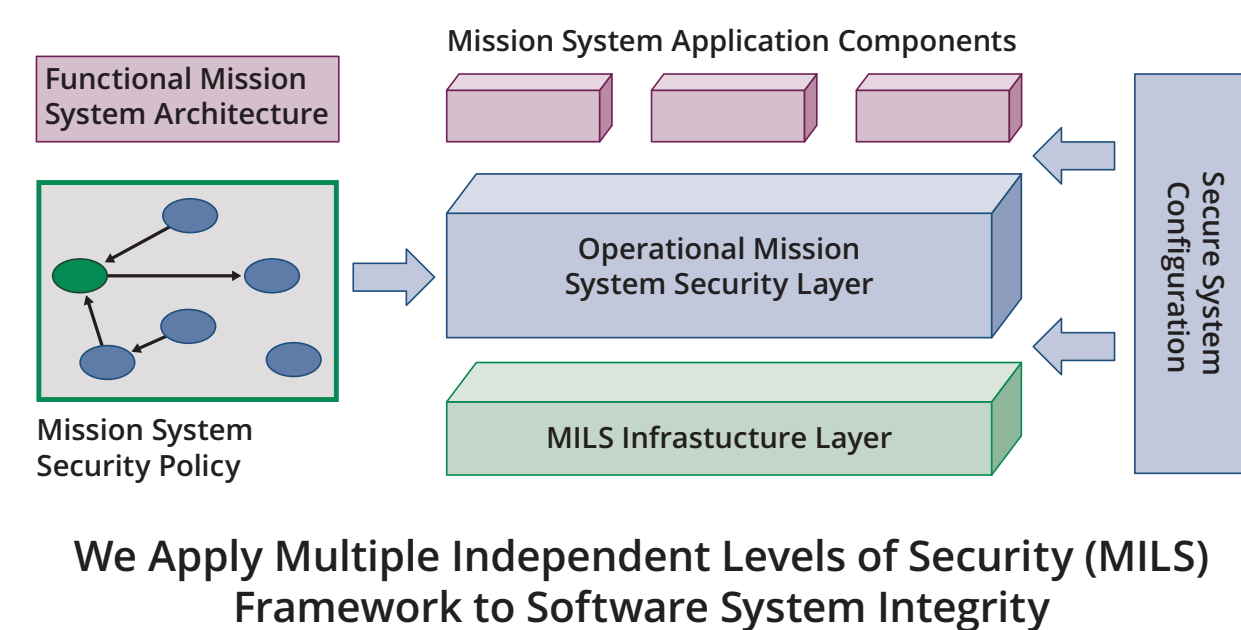


Automated Assurance of Security Policy Enforcement

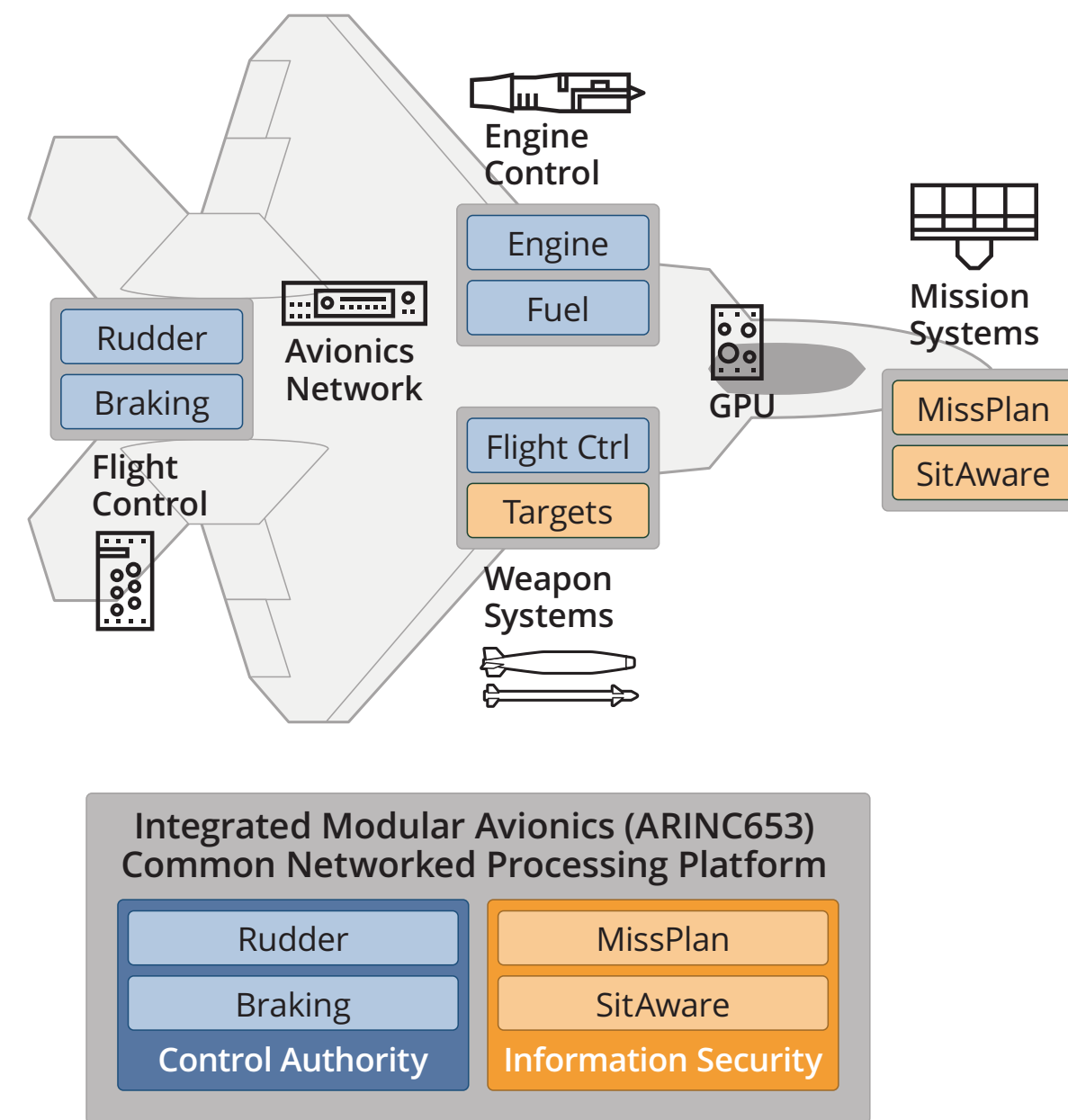
As safety-critical systems have become more connected, "closed" system assumptions are no longer valid and security threats affect safe system operation.

Virtual system integration and analysis of embedded software systems has been embraced by the safety-critical system community to address exponential growth in system development cost due to increased interaction complexity and mismatched assumptions in embedded software systems.

In this project, we demonstrate how the virtual system integration approach can be extended to address security concerns at the architecture level to complement code level security analysis.



Security Challenges as Safety-critical Systems Become Connected

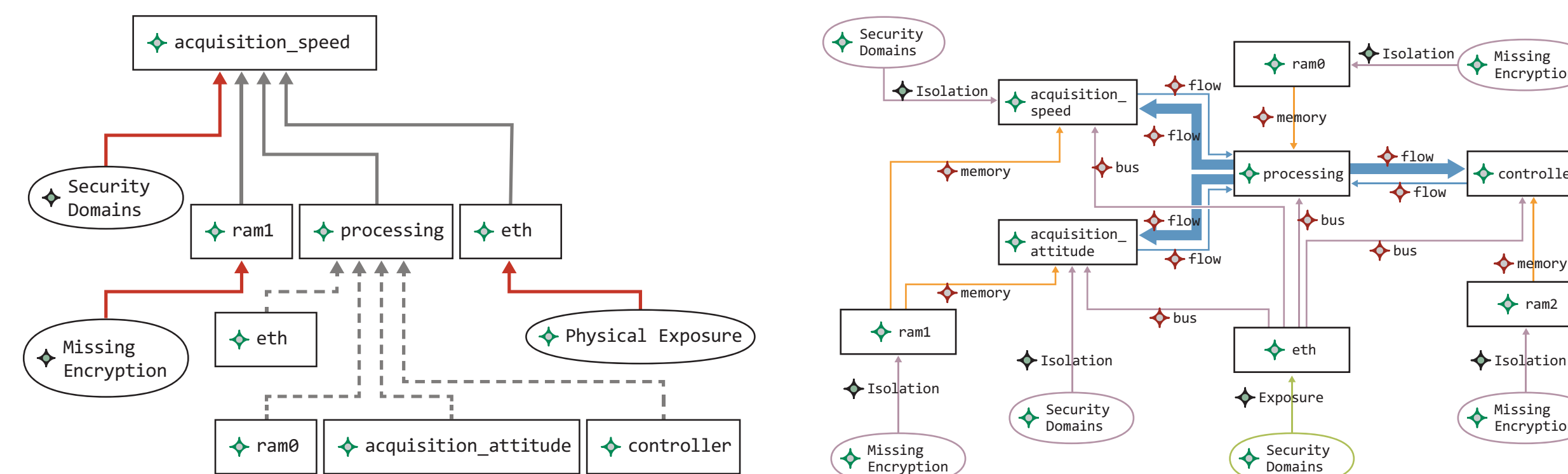


Our focus is on security policy specification and its enforcement

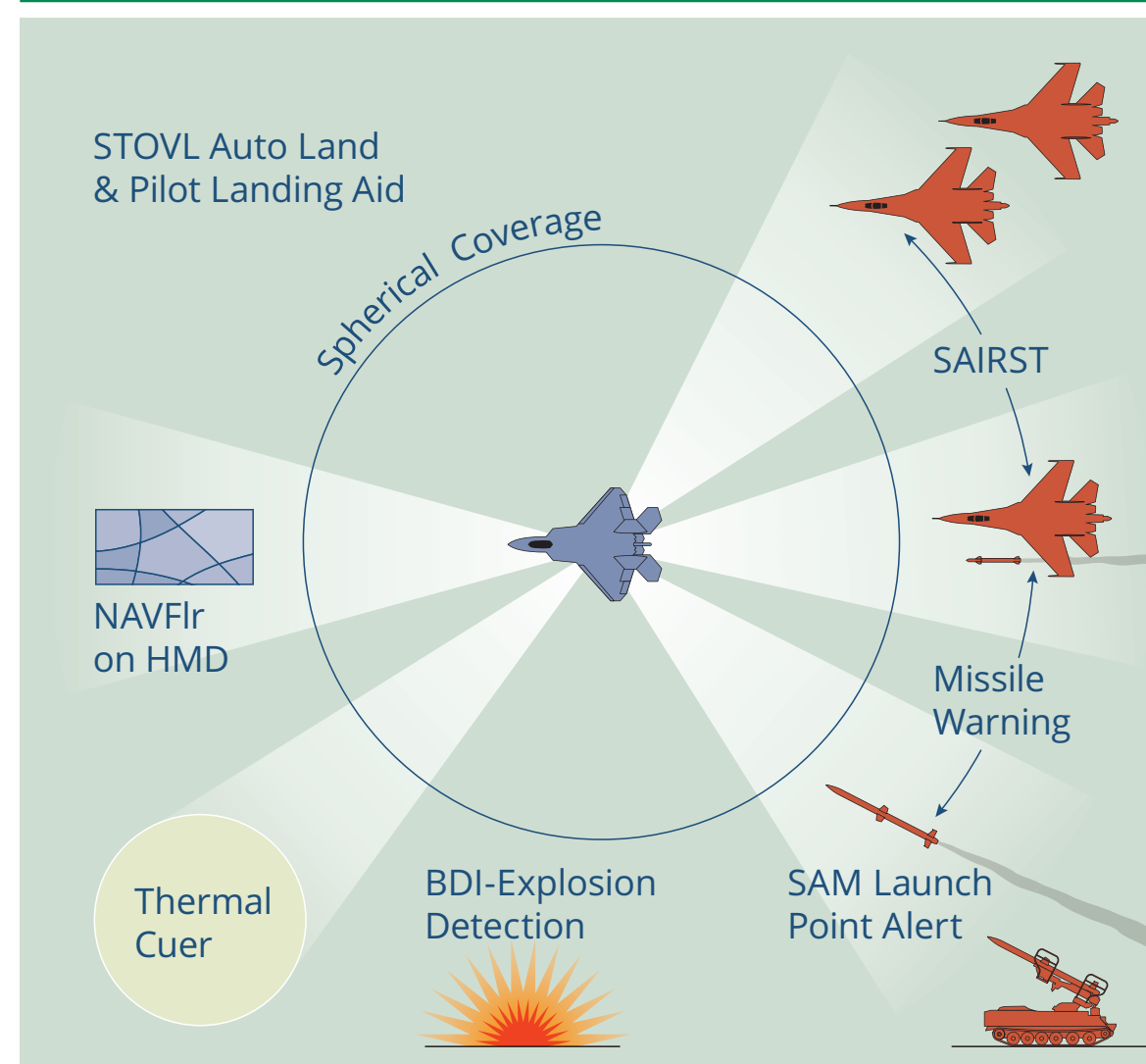
We utilize the SAE International Architecture Analysis & Design Language (AADL) industry standard to model and analyze embedded software systems. It includes an annex for fault modeling and analysis.

We analyze security policy specifications for consistency and gaps in flow constraints and isolation requirements.

We analyze the software system architecture for potential enforcement vulnerabilities due to incorrect deployment of security mechanisms.



From closed to connected systems



Security Attacks on External Channels and System Internal Vulnerabilities

Safety-critical avionics systems use partitioning to achieve fault isolation

Automated Assurance through Continuous Analysis of Potential Architecture Level Security Policy and Enforcement Vulnerabilities

We leverage the Architecture-Led Incremental System Assurance (ALISA) capability in the Open Source AADL Tool Environment (OSATE).

Executable verification plans identify how potential architecture level security vulnerabilities are addressed through model-based analysis.

- 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.

System case JeepSecurityCase: (S94 F9 T0 E0 tbd0 ELO TSO)

- Model JeepSecurityCase.JeepSecurityPlan(integration.attack)
 - Claim MILS_R5(integration.attack): MILS_R5: All non-verified components
 - Claim CWE131(integration.attack): CWE131: incorrect calculation
 - Evidence vaCWE131a (203 ms): check connections for correct timing
 - Evidence vaCWE131b (252 ms): Check that timing requirements are met
 - Claim CWE311(integration.attack): CWE311: Missing Encryption of Sensitive Data
 - Claim CWE805(integration.attack): CWE805: Buffer Access with Incorrect Length Value
- Subsystem cellular: (S4 F2 T0 E0 tbd0 ELO TSO)
 - Claim MILS_R0(cellular): MILS_R0: Components sharing a bus should have the same security level
 - Claim MILS_R1(cellular): R1: Components with different security levels use isolated memory regions
 - Claim MILS_R5(cellular): MILS_R5: All non-verified components
 - Claim CWE311(cellular): CWE311: Missing Encryption of Sensitive Data
 - Claim CWE805(cellular): CWE805: Buffer Access with Incorrect Length Value
 - Claim MILS_R6(cellular): R6: All communication that are not encrypted
- Subsystem internet: (S5 F1 T0 E0 tbd0 ELO TSO)
 - Claim MILS_R0(internet): MILS_R0: Components sharing a bus should have the same security level
 - Claim MILS_R1(internet): R1: Components with different security levels use isolated memory regions
 - Claim MILS_R5(internet): MILS_R5: All non-verified components
 - Claim CWE311(internet): CWE311: Missing Encryption of Sensitive Data
 - Claim CWE805(internet): CWE805: Buffer Access with Incorrect Length Value
 - Claim MILS_R6(internet): R6: All communication that are not encrypted
- Subsystem router_cel: (S3 F0 T0 E0 tbd0 ELO TSO)
- Subsystem car: (S62 F6 T0 E0 tbd0 ELO TSO)
- Subsystem attacker_cel: (S5 F0 T0 E0 tbd0 ELO TSO)
- Subsystem attacker_wifi: (S5 F0 T0 E0 tbd0 ELO TSO)
- Subsystem attacker_internet: (S5 F0 T0 E0 tbd0 ELO TSO)

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* 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 external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

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

DM17-0732

Automated Assurance of Security Policy Enforcement