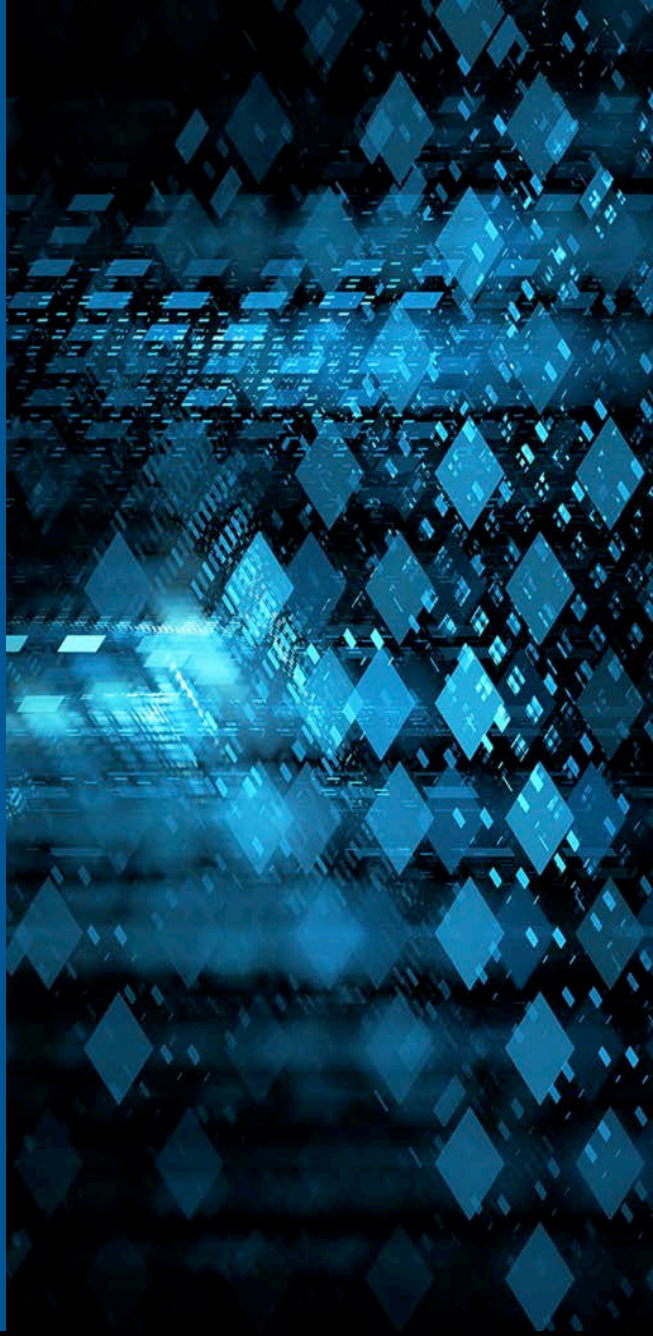
AADL Security Analysis Tools

Julien Delange, Min-Young Nam
Joseph Seibel

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003601

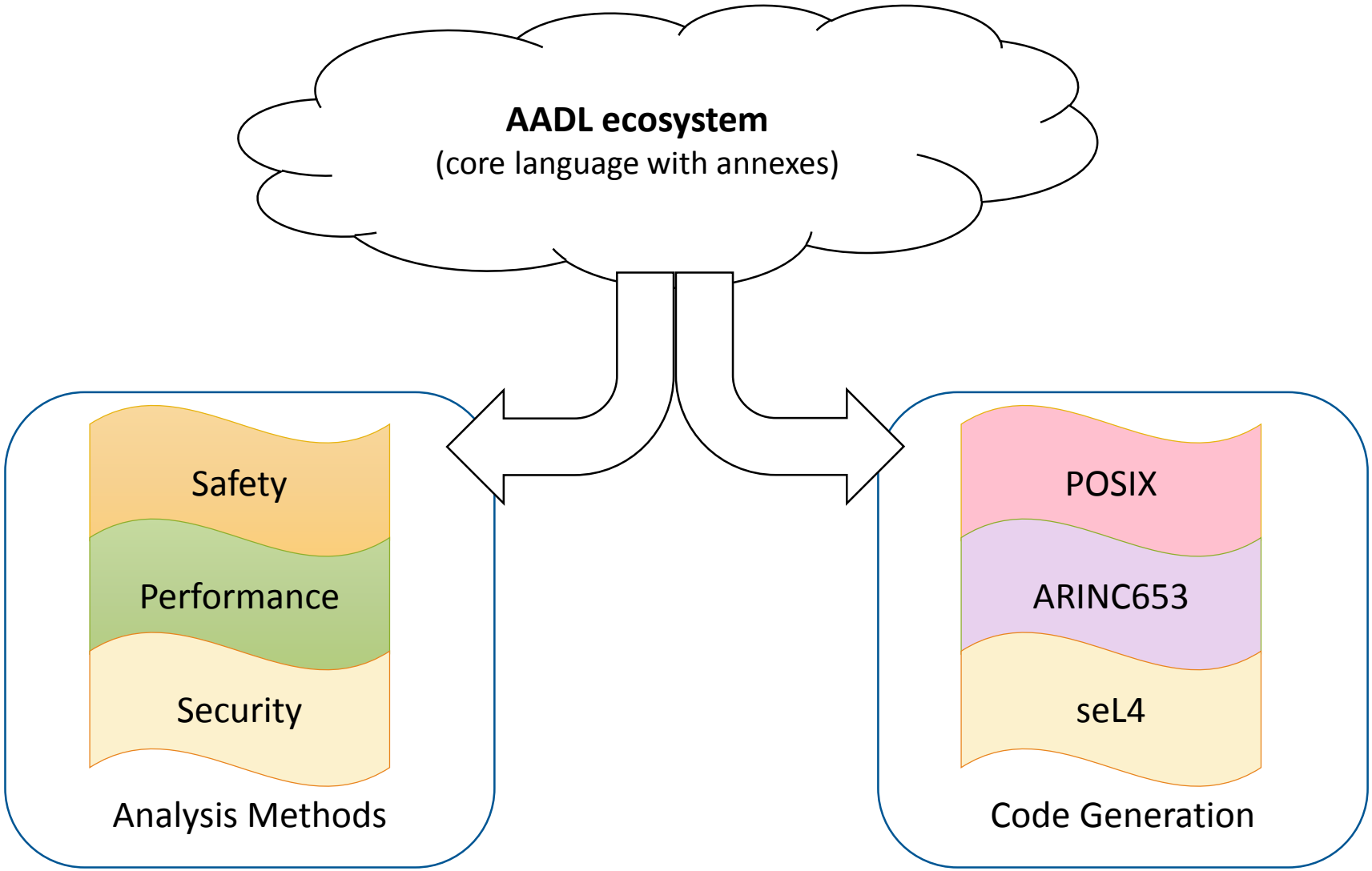
Agenda

Security Analysis Tools

Case-Study

Timeline and dissemination plan

Security Analysis Tools



New Capabilities

Attack Impact

Show vulnerabilities and their impact

Similar to the FMEA for security purposes

Attack Tree

Contributors (vulnerabilities) to a successful attack

Similar to FTA for safety purposes

Code Generation for seL4

Formally verified kernel focused on security

Automate generation of configuration & deployment code

Implementation Concerns

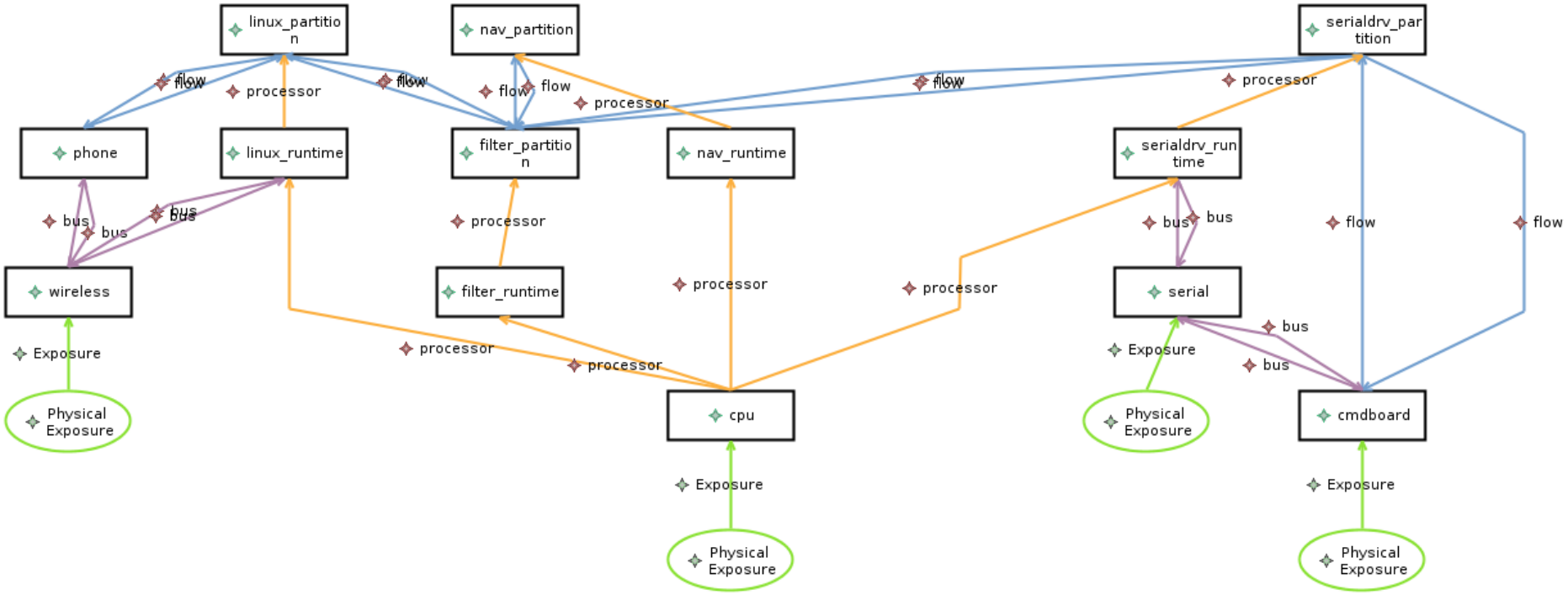
Attack Impact & Attack Tree

- Built-in support in Eclipse
- Graphical representation with Sirius
- Automatic Generation of AI and AT from AADL models

seL4 code generation

- Leverage Xtend code generation template
- Rely on CAmkES (seL4 ADL)

Attack Impact Analysis Example



Drone case-study goals and objectives

Model & Analyze a cyber-physical system with AADL

- Annotate the AADL model with new security properties
- Demonstrate use of security analysis tools

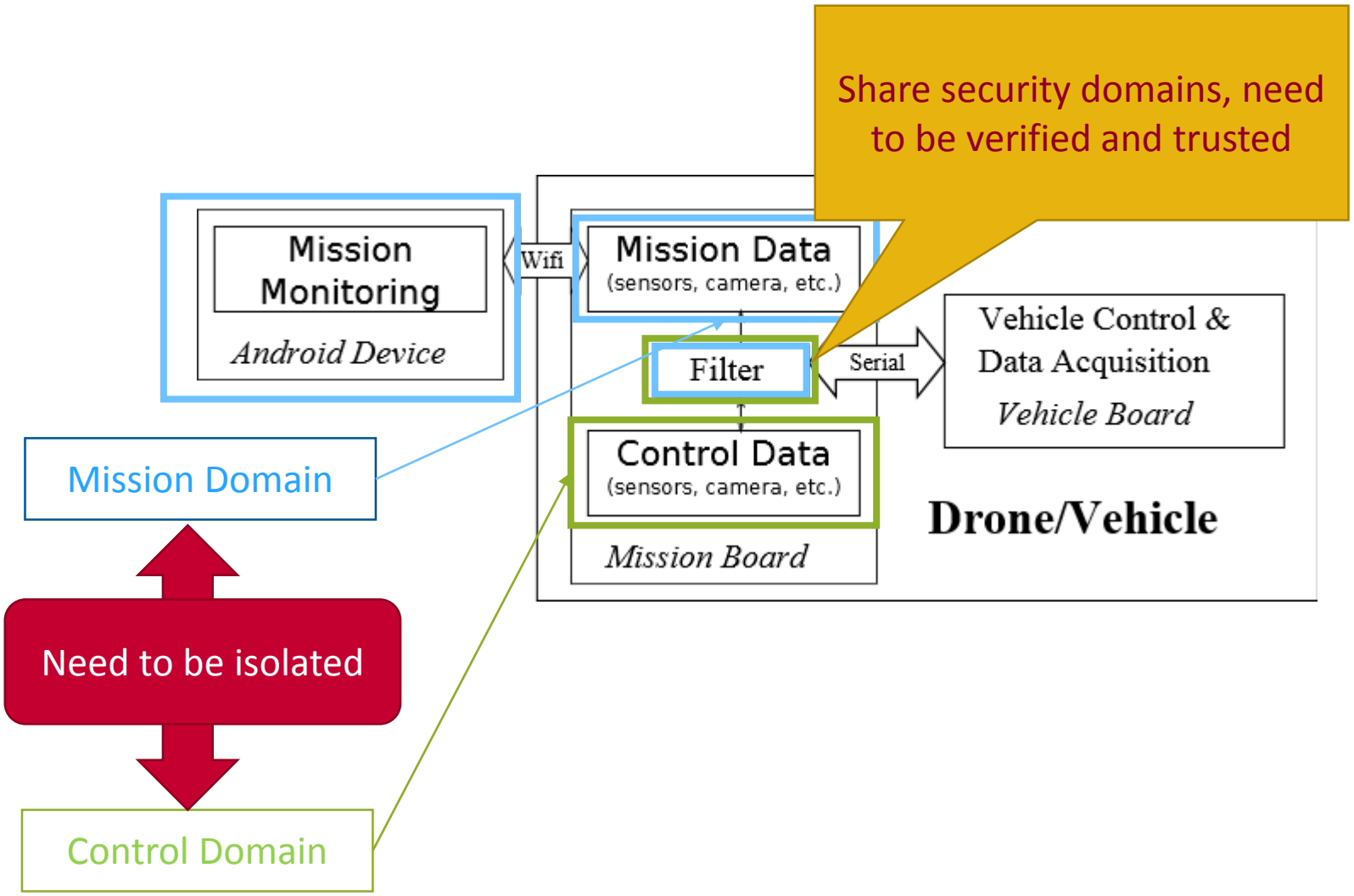
Generate runtime code for a secure runtime

- Automate code production for seL4

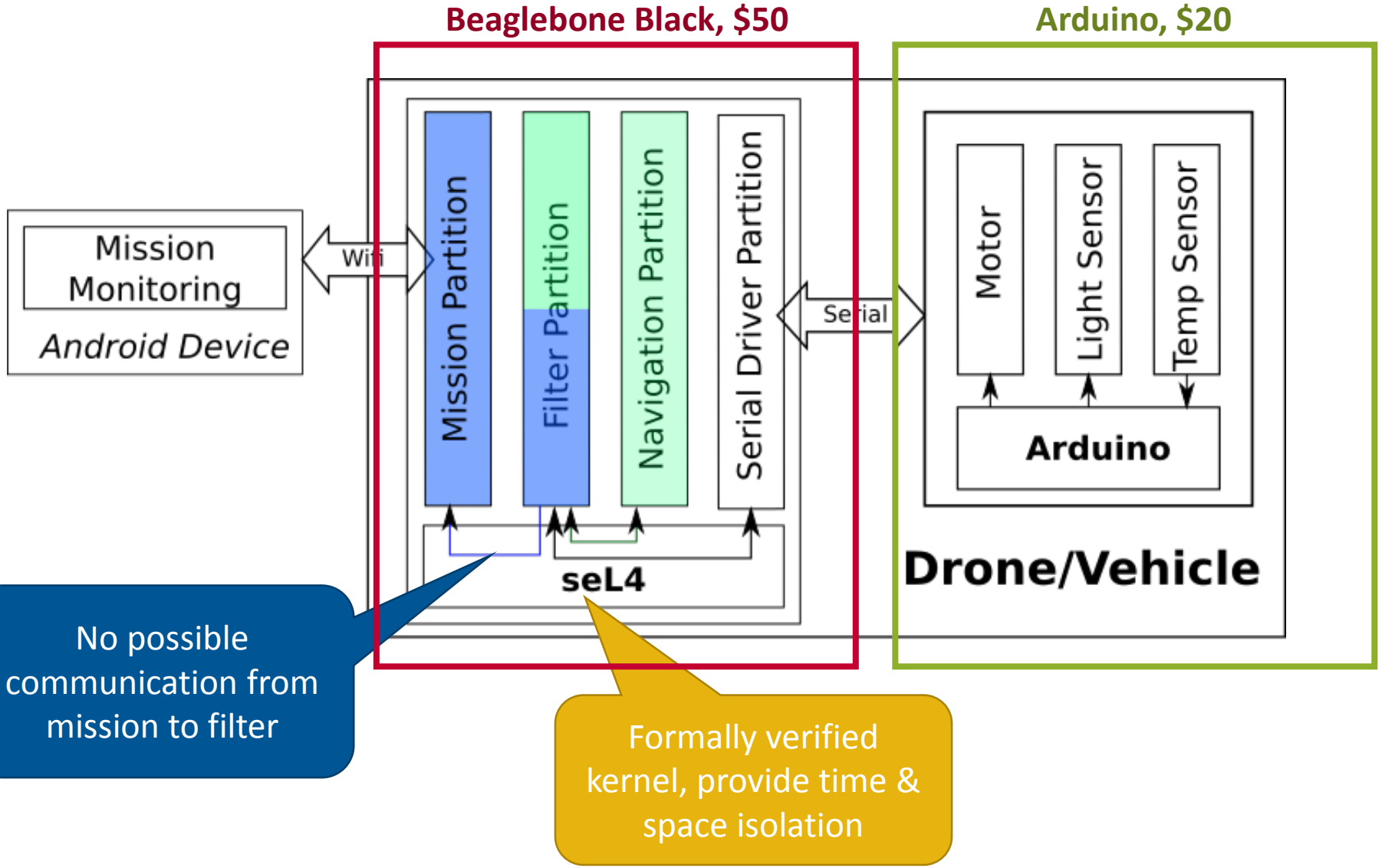
Virtual Integration Education Platform

- All tools are available publicly, EPL or BSD license
- Low-cost platform (total ~ $100)

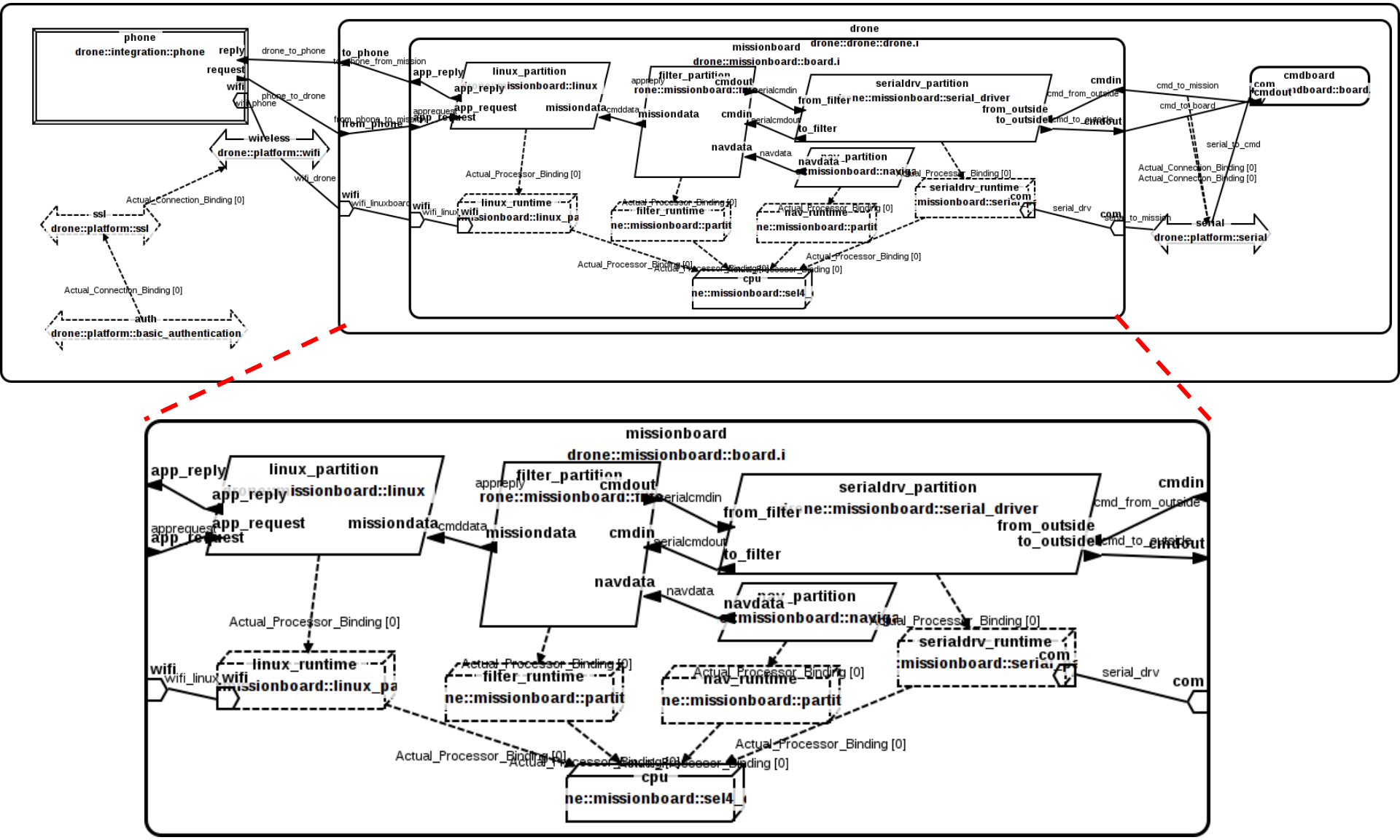
Drone case-study – functional overview



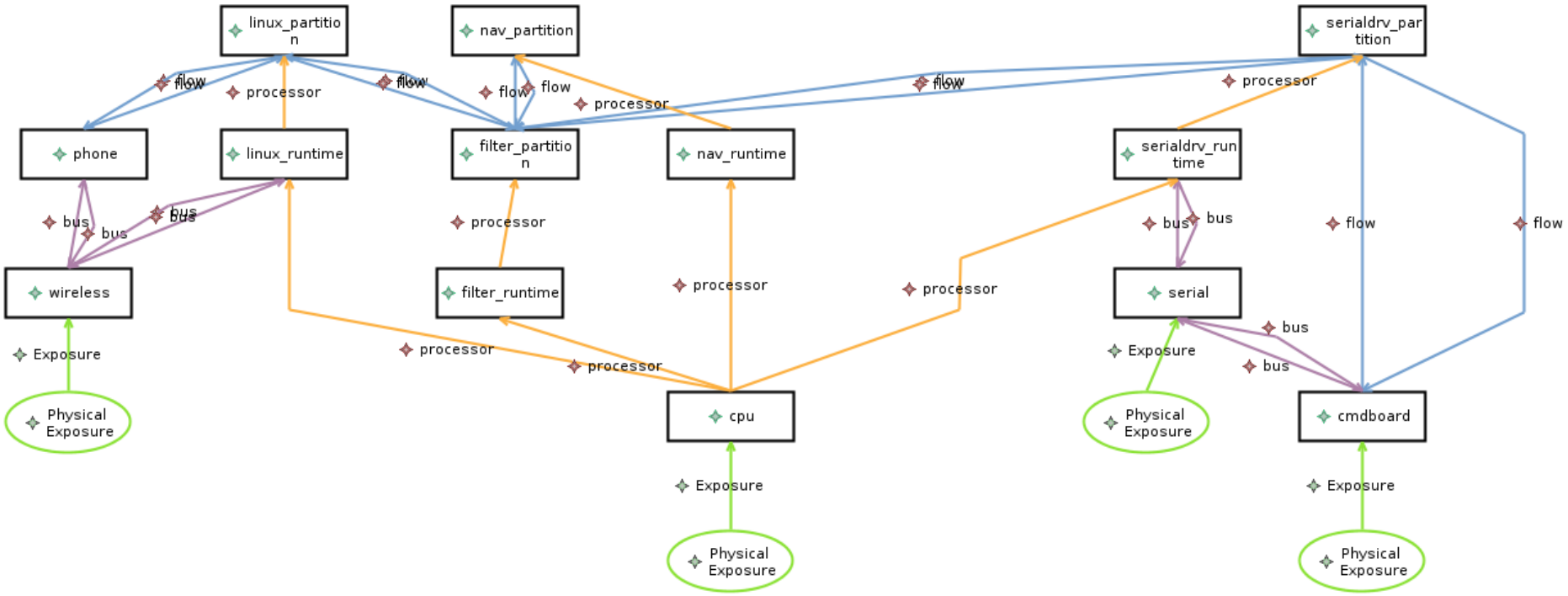
Drone case-study - implementation



Drone AADL model



Drone – Attack Impact



Drone – Code Generation Status

Able to generate functional code

- Support for beaglebone
- Support for x86, beaglebone & Nvidia Tegra K1

Need runtime support for serial and wifi drivers

- SEI is investing in seL4, developing driver support
- Planning to support beaglebone later this year

Dissemination plan

May 2016

Presentation of security annex and tools

Tool improvements

June 2016

Tool improvements

Legal agreements

July 2016

Publication on SEI github

Julien Delange

CMU-SEI

4500 5th avenue

Pittsburgh, PA15213

+1-412-268-9652

jdelange@sei.cmu.edu