

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

DM-0003601



Agenda



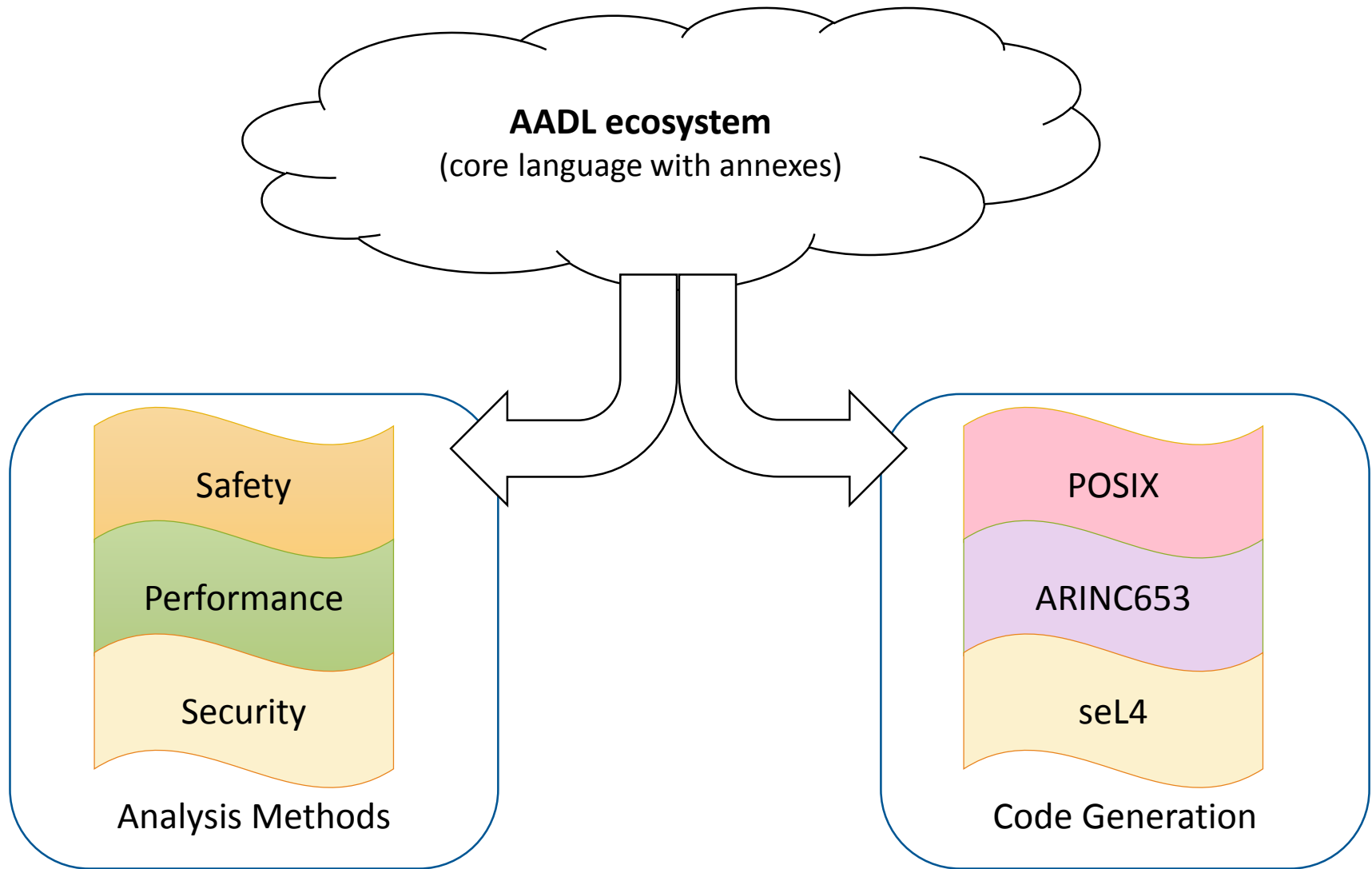
Security Analysis Tools

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

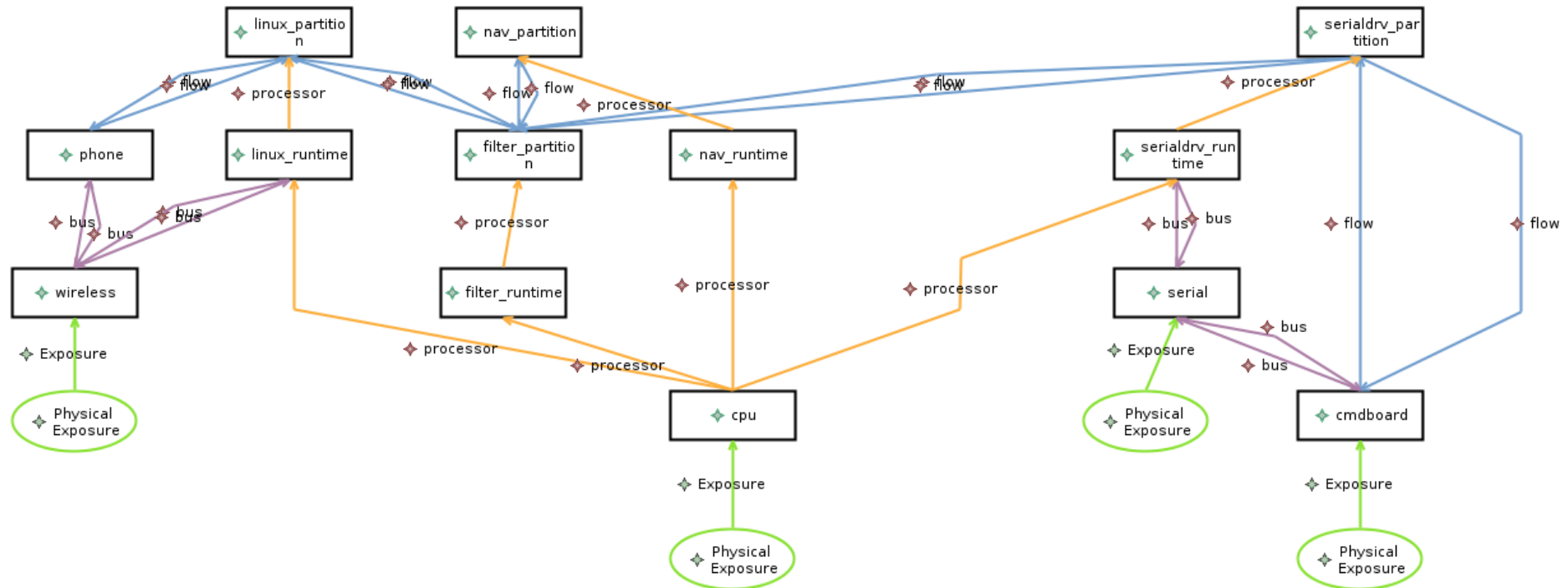
seL4 code generation

- 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

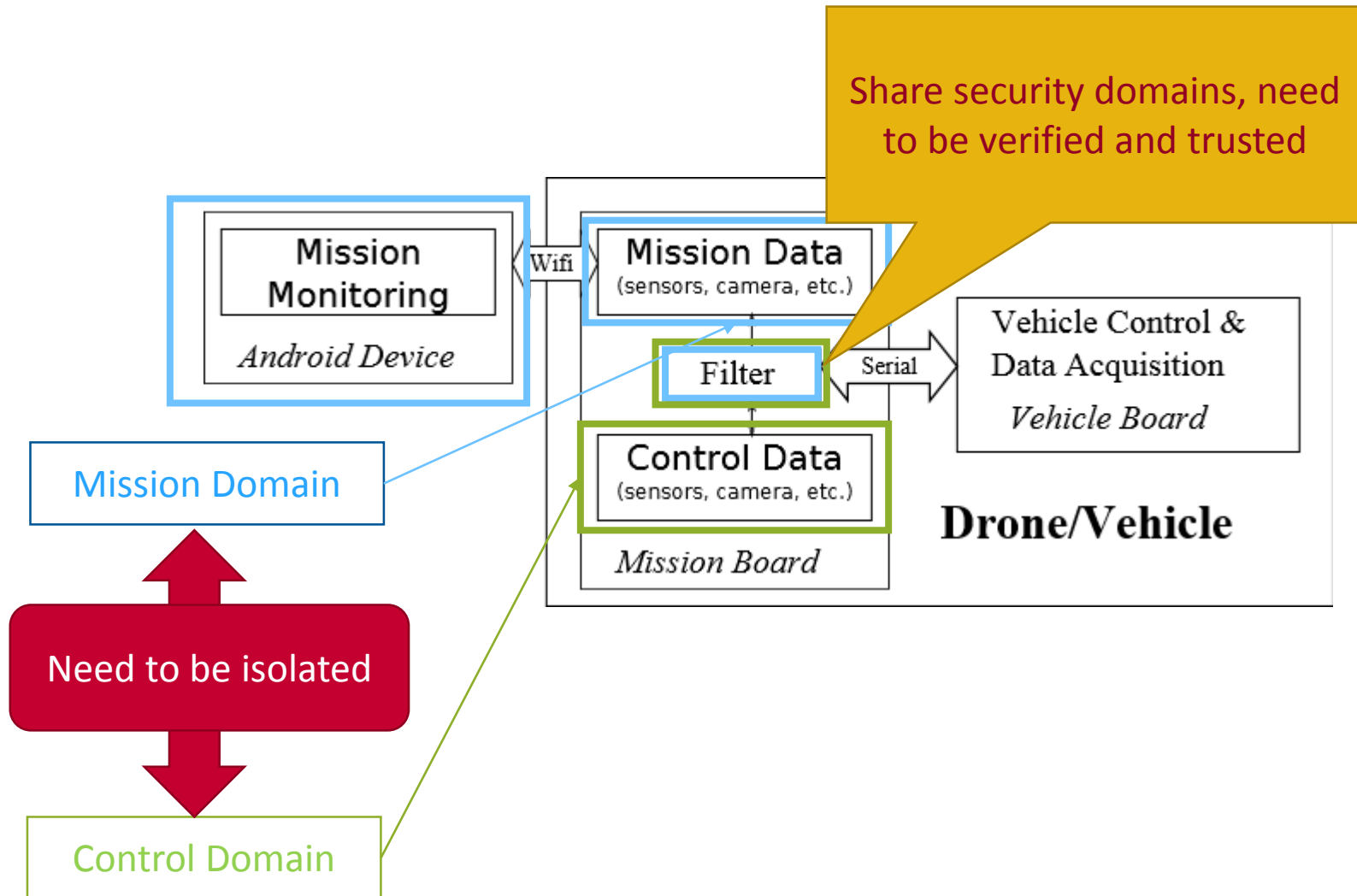
Automate code production for seL4

Virtual Integration Education Platform

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



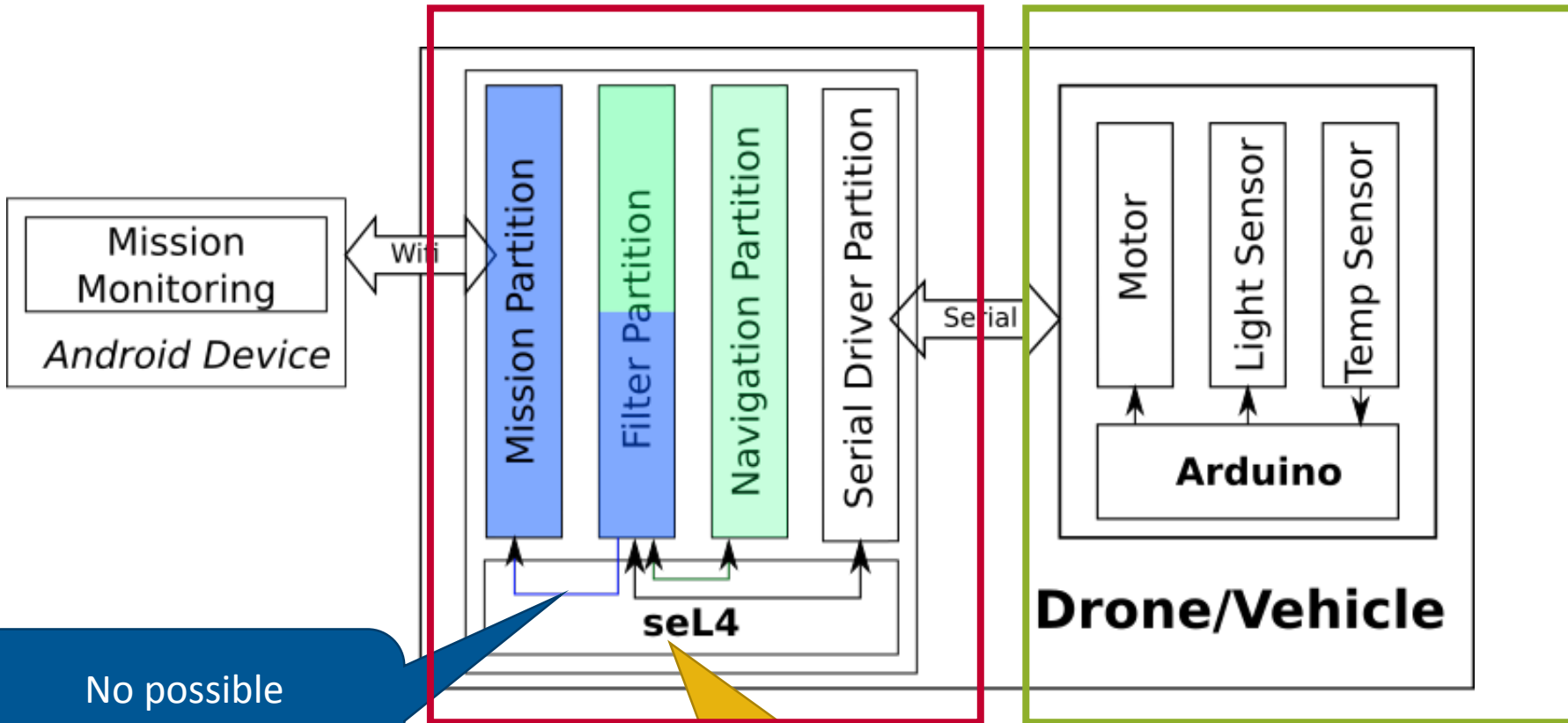
Drone case-study – functional overview



Drone case-study - implementation

Beaglebone Black, \$50

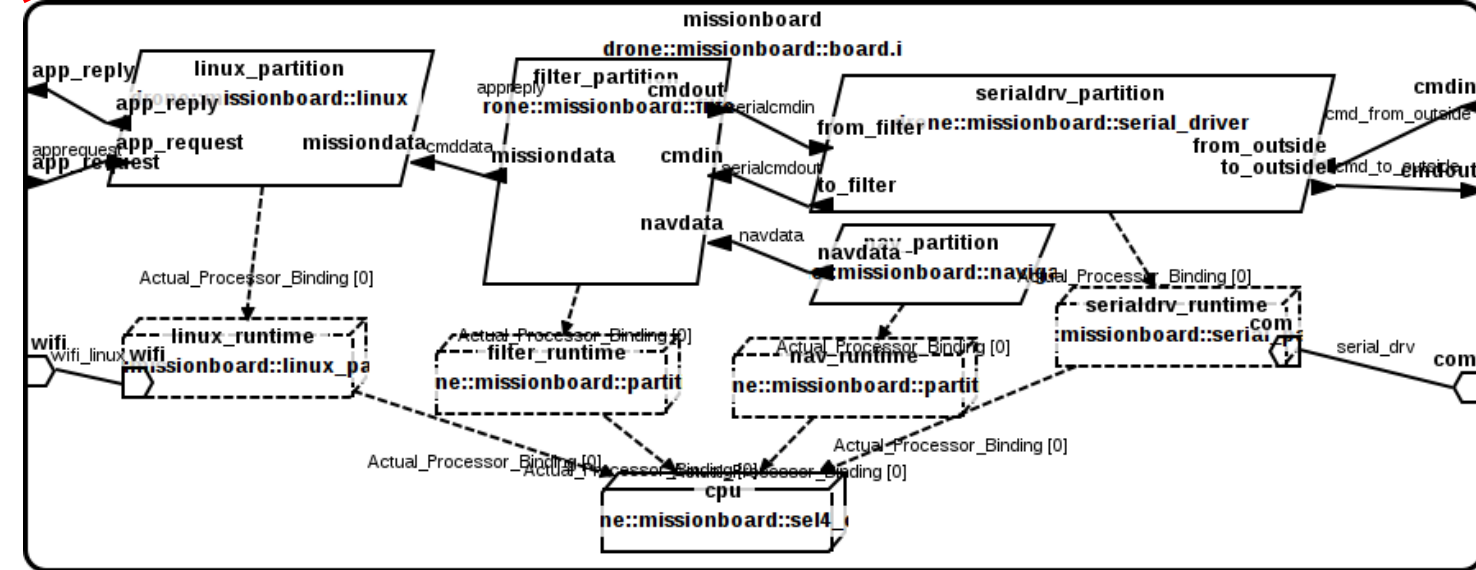
Arduino, \$20



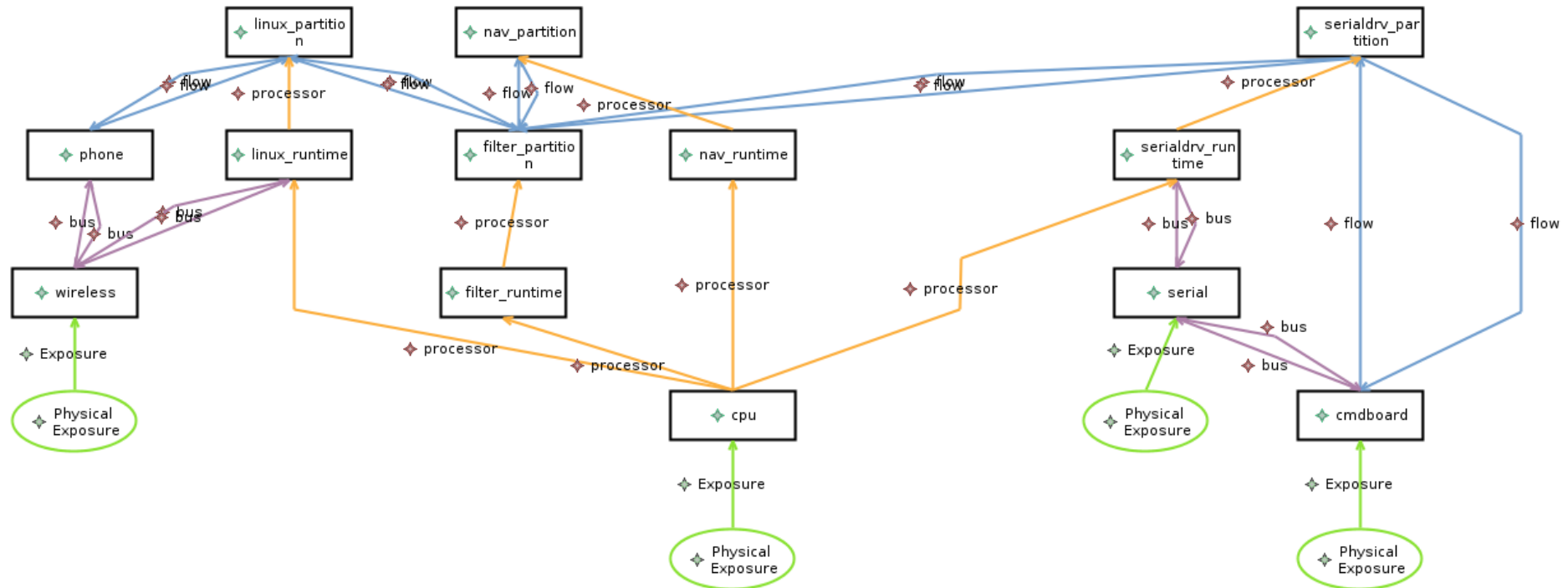
No possible communication from mission to filter

Formally verified kernel, provide time & space isolation





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