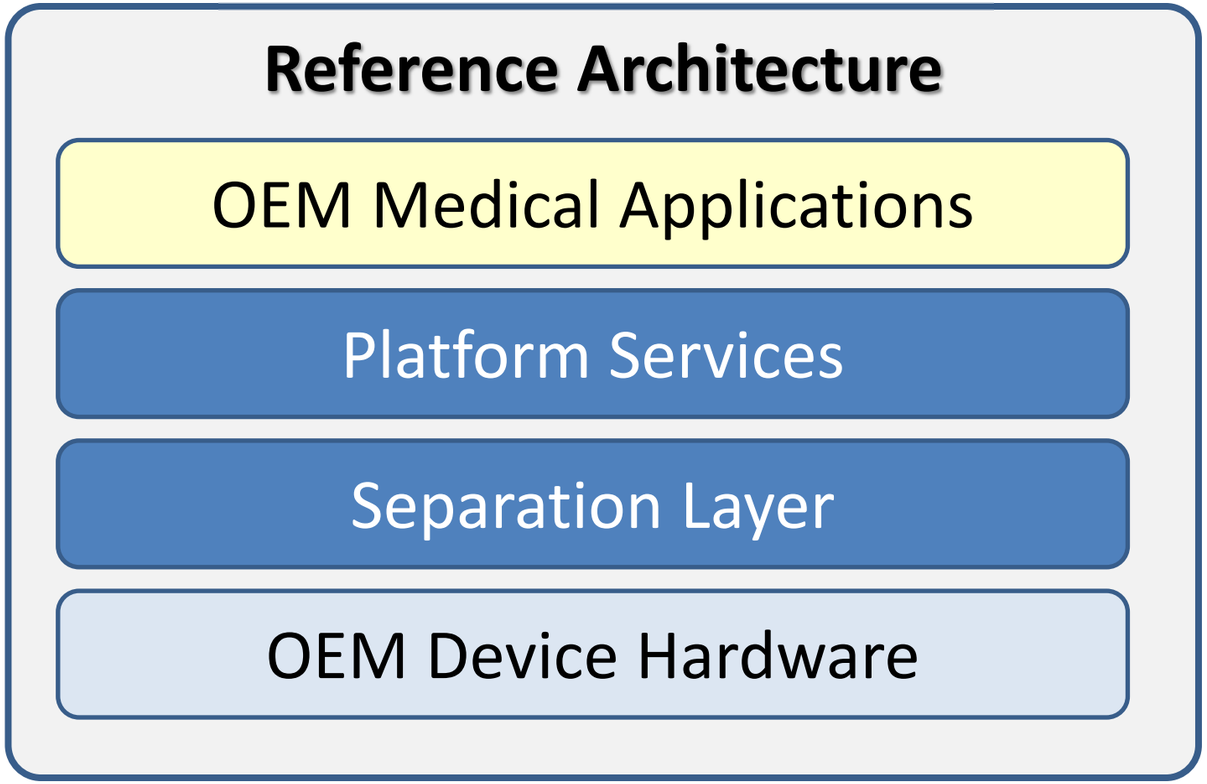
# Safe and Secure Embedded Device Reference Architecture

Todd Carpenter, Dr. Danielle Stewart, Adventium Labs

# Reference Architecture Concept

- **Motivation**: Security issues are getting worse
- **Approach**: Provide a reference architecture so medical device teams can get a solid start
- **Artifacts:**
  - Educational material
  - Requirements and designs
  - Model based tools for analysis and configuration
  - Example HW and SW



# Healthcare Needs Cyber Security

- Successful attacks on healthcare systems and medical devices include:
  - Data breaches to steal patient and business information
  - Ransomware and selling short to directly profit from security vulnerabilities in medical devices
  - Live hospital network attacks to increase sales
- Medical device companies need suitable technology and expertise:
  - 80% of device manufacturers have 50 or fewer employees
  - Expert **embedded systems security developers** are in short supply
- Typical development processes do not treat safety and security as first-class concerns

**Attackers target medical devices to bypass hospital security**
http://www.csoonline.com/article/2931474/data-breach/attackers-targeting-medical-devices-to-bypass-hospital-security.html

**IT security company uses live hospital network to promote sales**
https://arstechnica.com/security/2017/04/security-vendor-uses-hospitals-network-for-unauthorized-sales-demos/

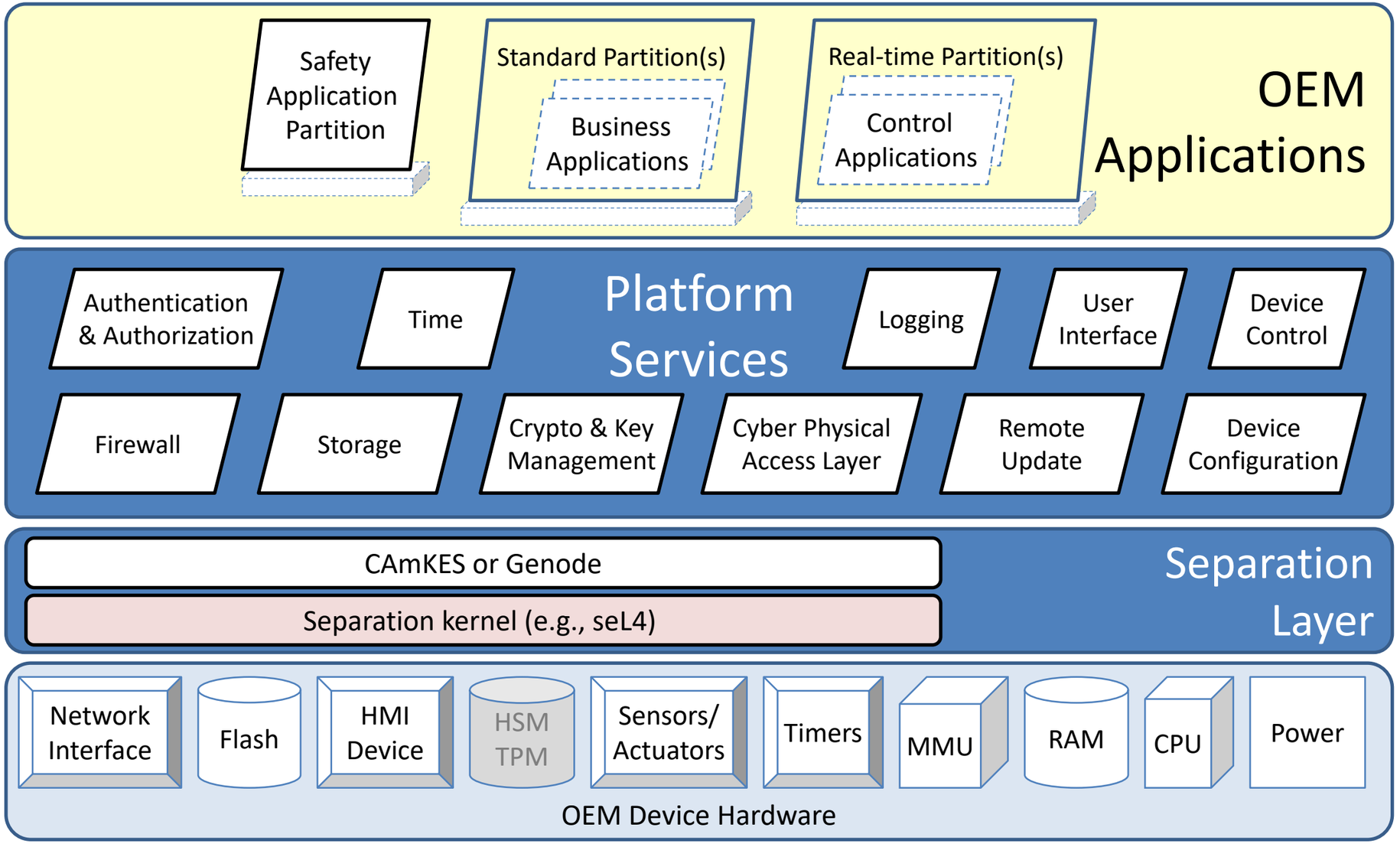
**WannaCry Ransomware Encrypted Hospital Medical Devices**
http://www.hipaajournal.com/wannacry-ransomware-encrypted-hospital-medical-devices-8811/

**Stock shorted on heart device hacking fears; shares drop**
http://www.reuters.com/article/us-stjude-cyber-idUSKCN1101YV

# ISOSCELES Separation Architecture

**Key Principles:**

- Time and Space Separation
- Least Privilege
- Minimal Complexity
- Trust Relations
- Cryptographic Basis
- Model-based Engineering
- Models of Correctness



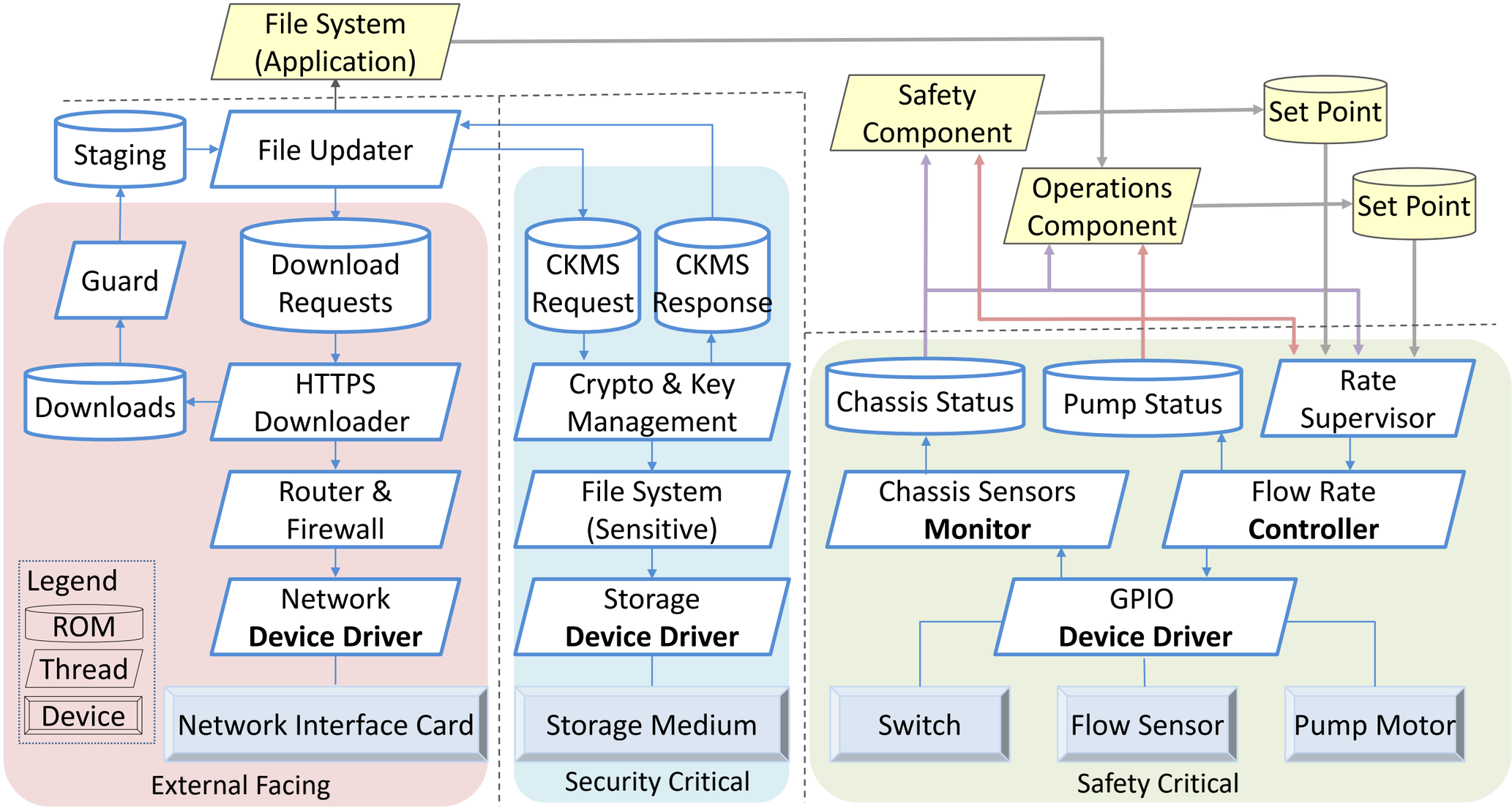

Disaggregated architecture supports safety and security as well as diverse applications

# Example Mixed Criticality System

**Example Embedded System: Infusion Pump**

Multiple Enclaves:

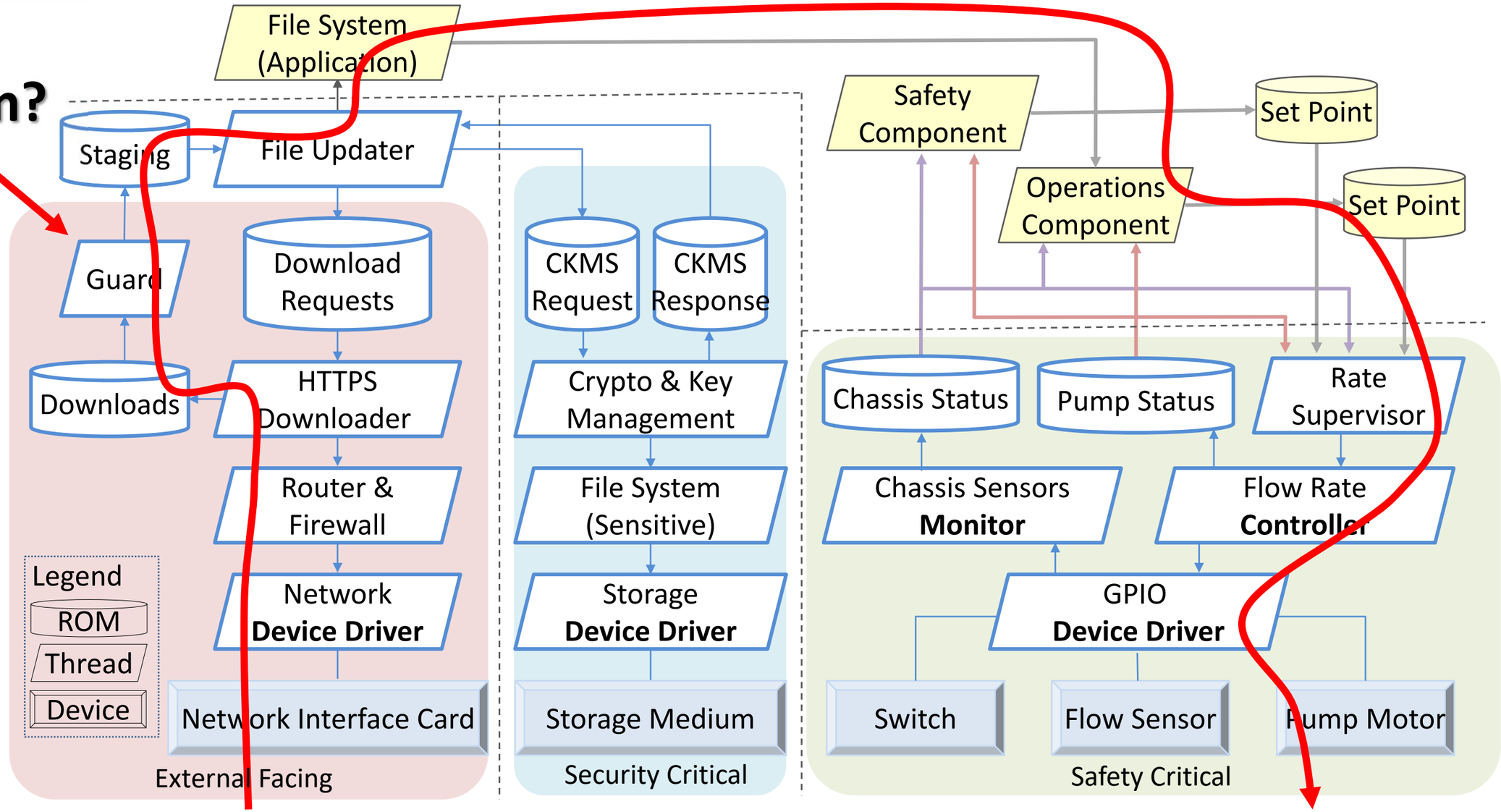
- External Facing
- Security Critical
- Safety Critical




Certifying entire Mixed Criticality Systems to the level of the highest criticality component is cost prohibitive

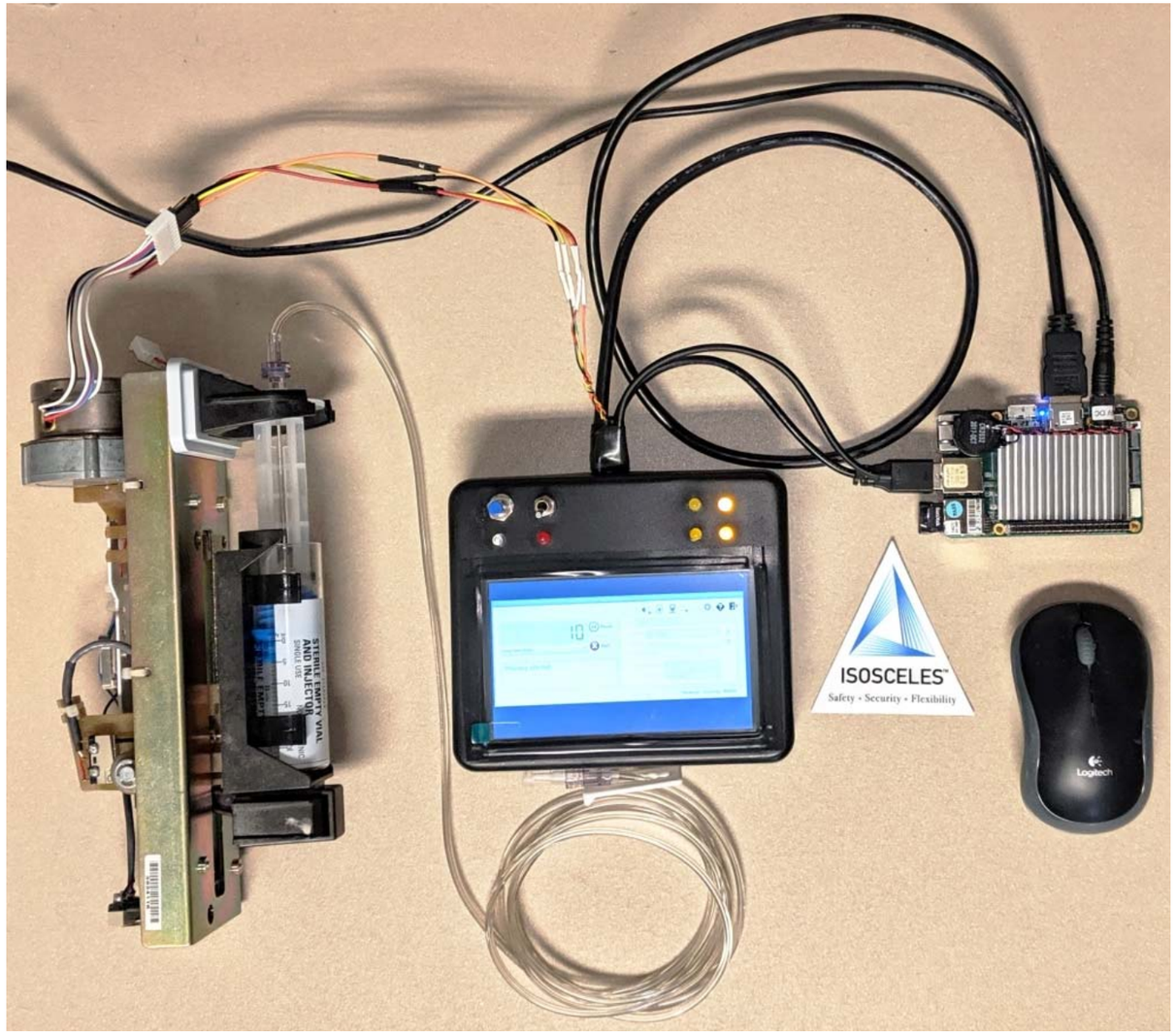
# seL4 Brick Walls vs Information Flow

**Bridge of Khazad dûm?**




Need: Safe and Secure integration of interconnected enclaves

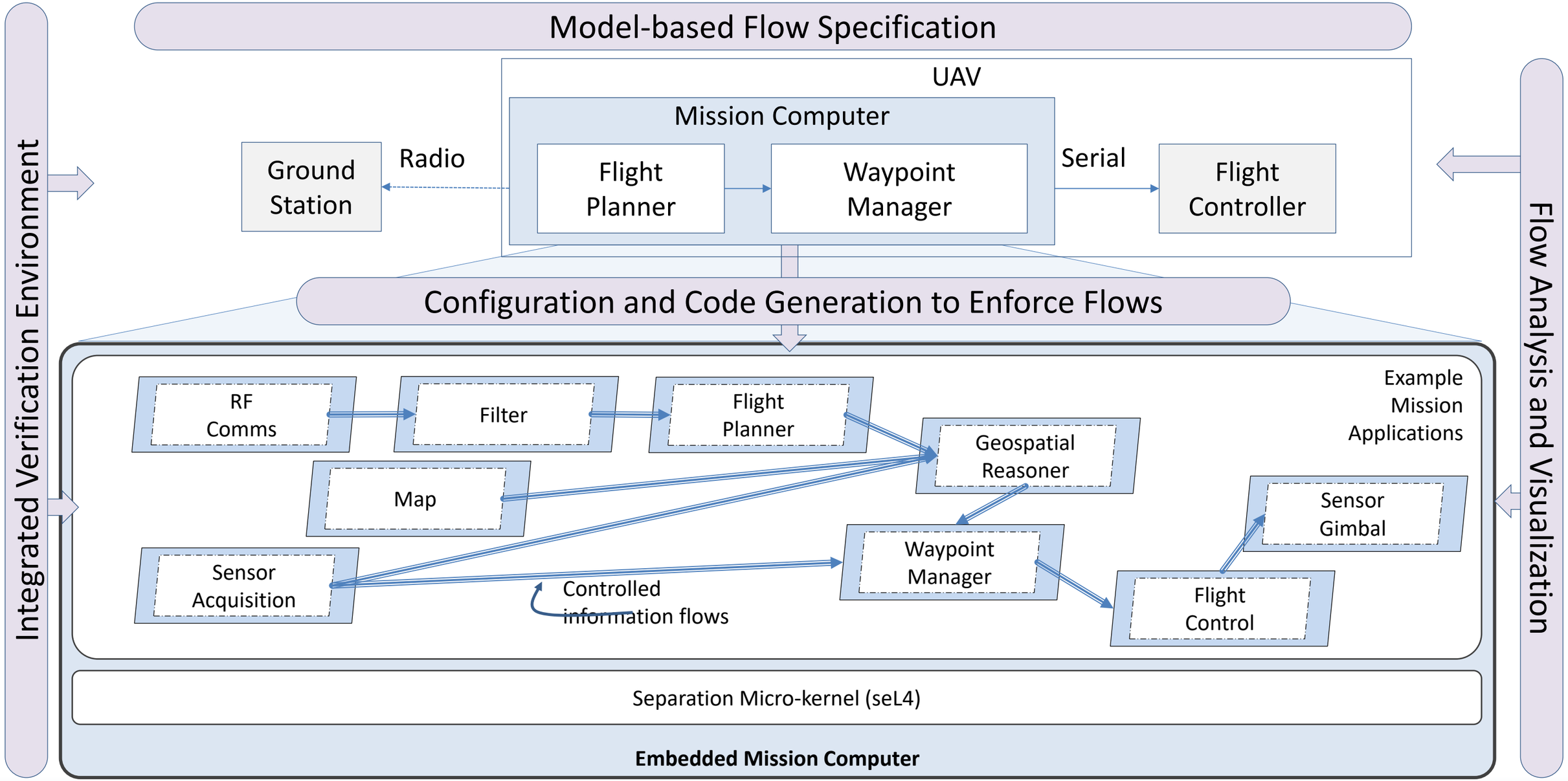
# ISOSCELES Demonstrator: Infusion Pump




- Prototype infusion pump includes
  - Timers, HDMI GUI, mouse, GPIO, networking, file system storage
  - Secure logging, remote drug library update, network time protocol
- Highly disaggregated platform – no VM
- Genode (18.08) on seL4 or NOVA
- seL4 total image size: ~47MB
- Intel x86, Intel Atom, QEMU, VirtualBox
- Auto-generated C++ for safety-critical component
- Auto-generated Genode configuration from AADL
- Continuous integration development environment

ISOSCELES is a safe and secure IoT device platform demonstrator

# Major Toolchain Components



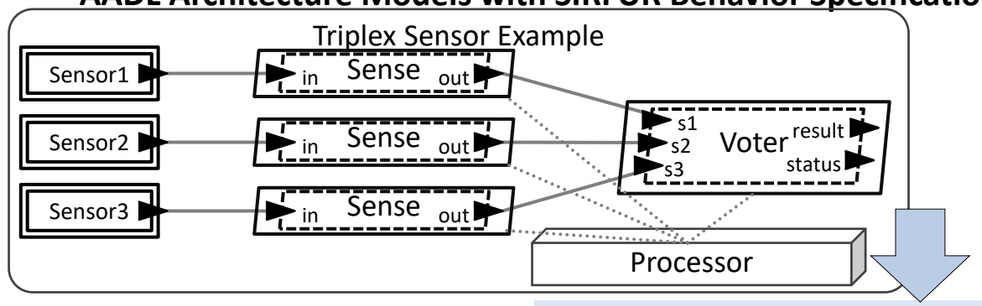
# Integrated Verification Environment

Engineering Models

Verifiable Slang Code

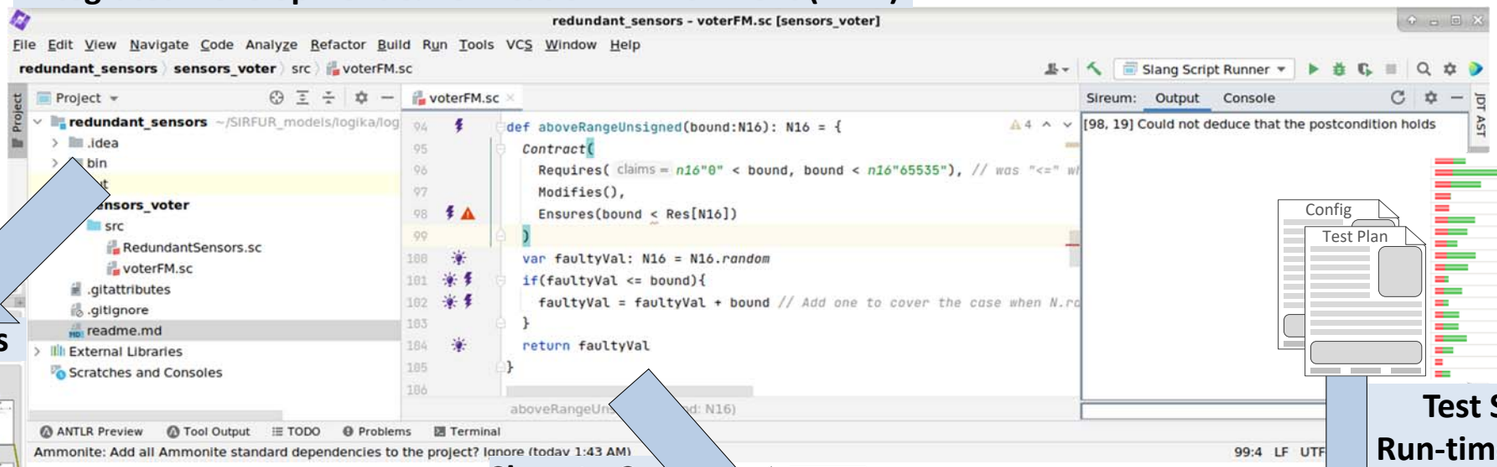
Verified Kernel Deployments

**AADL Architecture Models with SIRFUR Behavior Specifications**

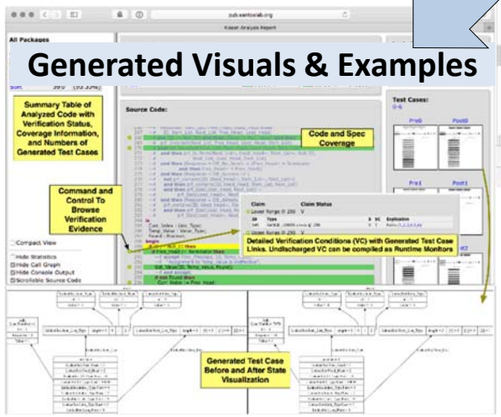



- Specification Translation
- Implementation Verification
- Code Generation
- Kernel Configuration (via HAMR)

**Integrated Development & Verification Environment (IDVE)**

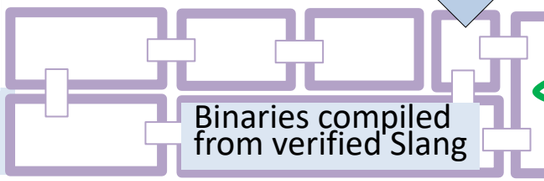



**Generated Visuals & Examples**




**Slang to C Compilation**


**Kernel Configuration**



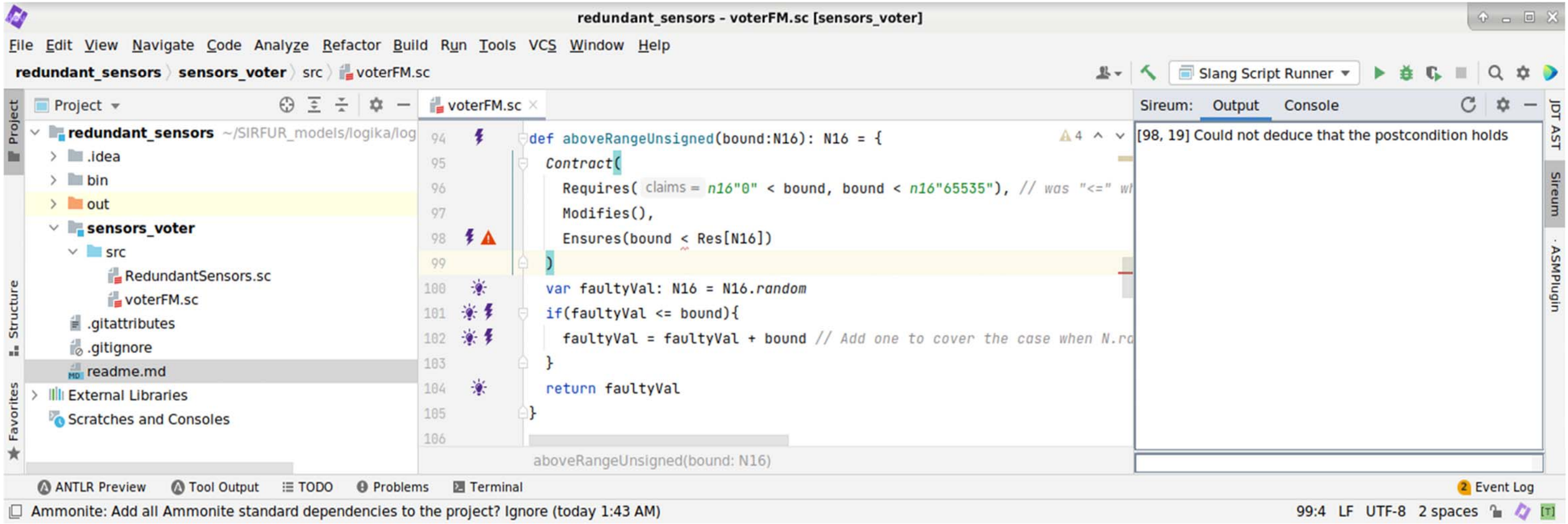

**seL4 Verified Micro-kernel**



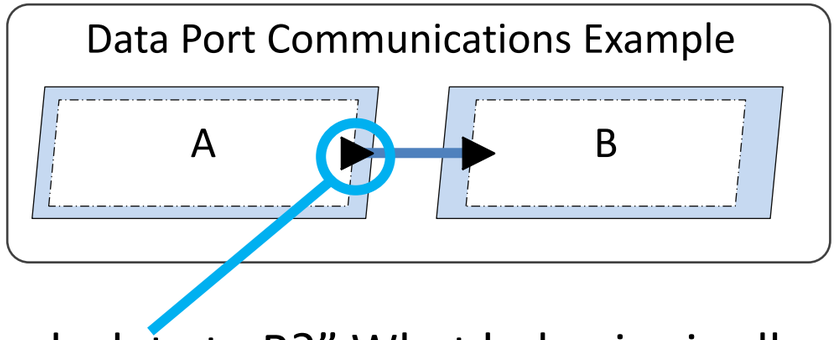

**Test Suites & Run-time Monitors**

**Thread and Communication Patterns**

# IVE Screenshot



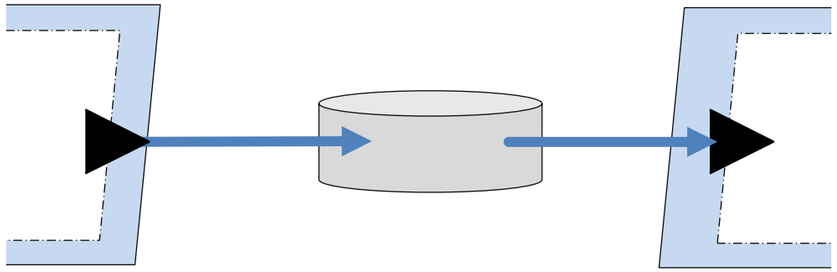
# AADL to seL4 Communications




What does it really mean when “A sends data to B?” What behavior is allowable?

Goal: Connections are unidirectional – no feedback, no mixed control/dataflow, non blocking, no additional info other than intended (aka “as specified”) channel

Implemented as seL4 shared memory



No RPC, which mixes control-flow concepts

Writer (sender) has write access, and writing occurs during writer’s scheduled execution time
Reader (receiver) has read access, and reading occurs during reader’s scheduled execution time
Reads and writes are non-blocking

During DARPA CASE, we developed space and time secure data and event port communications

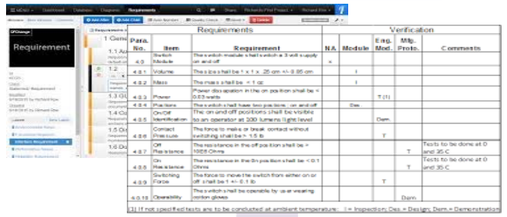
# Example Models

- Patient Controlled Analgesic (PCA) Pump
- Isolette
- Simple Unmanned Aerial Vehicle (UAV)
- Educational and test micro-examples

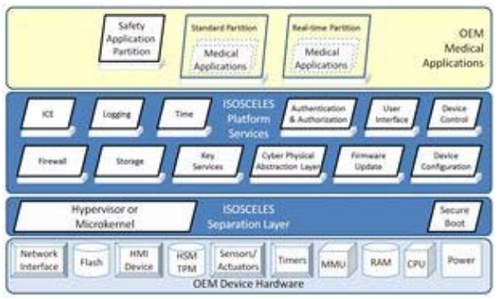
We use these models to inform our research, test tools and techniques, and demonstrate capabilities

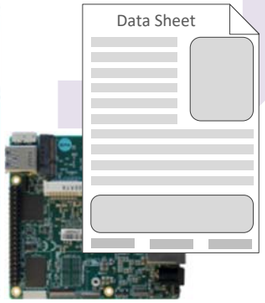
# Model-Based Workflow

Device Requirements



Platform Assets



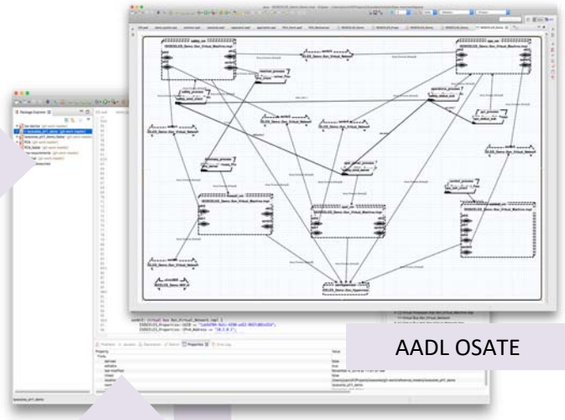

Risk Management (Safety, Security, Reliability)

Assurance Cases V & V Evidence

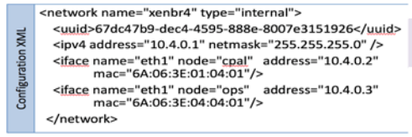
Regulatory Artifacts

Architecture Specification

- Information Separation
- Utilization
- Latency
- Risk Management Framework

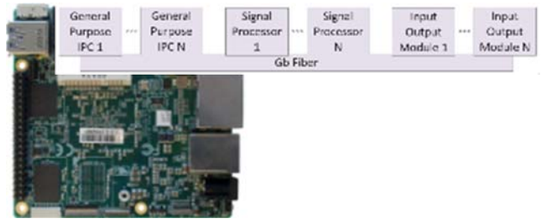


AADL OSATE




Platform Configuration Data61 CAmkES (genode)

Platform Deployment & Configuration Framework




Platform Run-Time Environment

Model-based tools support platform analysis and configuration

# Resources

**Open Source:**

- seL4 Foundation: https://sel4.systems/Foundation/home.pml
- Open Source AADL Tool Environment: https://osate.org/
- Kansas State Sireum: http://sireum.org/

**Commercial:**

- Adventium CAMET (and ISOSCELES): https://www.adventiumlabs.com/camet-tools
- HENSOLDT TRENTOS: https://hensoldt-cyber.com/trentos/