Intrinsically Secure, Open, and Safe Cyber-physically Enabled, Life-critical Essential Services (ISOSCELES)

ACSAC 2016

Todd Carpenter
Chief Engineer
todd.carpenter@adventiumlabs.com

This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency (HSARPA), Cyber Security Division (DHS S&T/HSARPA/CDS) BAA HSHQDC-14-R-B0005, the Government of Israel and the National Cyber Bureau in the Government of Israel via contract number D16PC00057. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security, the U.S. Government, the Government of Israel or the National Cyber Bureau in the Government of Israel.

Adventium Labs

We solve hard problems by blending:

- System Engineering
- Automated Reasoning
- Cyber Security

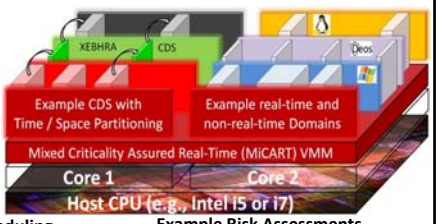
We perform R&D for:

- DHS
- DoD
- NASA
- NIH & Med-tech
- NSF

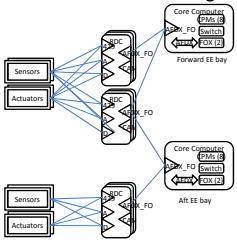
We transition results to:

- Industry
- Open-source community
- Education
- 100/100 DoD commercialization score

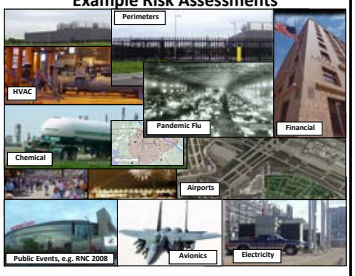
Mixed-criticality systems



Aircraft-wide scheduling



Example Risk Assessments



Andamio Games · Magrana SERVER · FASTAR · EVALFASTER® · STEAF

ISOSCELES Team

Adventium Labs

- Todd Carpenter – 25+ years designing safety and security critical systems including avionics, industrial control, and medical devices.
- Expert staff supporting medical devices, cybersecurity, safety critical systems, architecture modeling and development, enterprise security.

Kansas State University

- Dr. John Hatcliff – Safety critical model-based medical device design.
- Dr. Eugene Vasserman – Medical device security.

University of Michigan

- Dr. Kevin Fu – Medical device security evaluation.

Recent headlines

The Cybercrime Economy

Hospital network hacked, 4.5 million records stolen

Attackers targeting medical devices to bypass hospital security

MEDICAL CYBERCRIME: THE NEXT FRONTIER

Why Would Chinese Hackers Steal Millions of Medical Records?

Hacker Attacks on Healthcare Providers Jump 600 Percent

Why Your Medical Records Are No Longer Safe

Ransomware

Selling Short

Your medical record is worth more to hackers than your credit card

Anthem data breach could cost company billions

Insurance company tells hospitals: we shouldn't pay if you're careless with patient data

Industry Needs

80% of device manufacturers have 50 or fewer employees.

https://www.selectusa.gov/medical-technology-industry-united-states

- Focused on therapy and diagnostic innovations.
- Start-ups typically don't have the resources or knowledge to build in security from scratch.
- Regulators are asking for evidence that security has been designed in.

Need tools & templates to create a safe & secure base.

Large device manufacturers have demonstrated poor security knowledge with their fielded devices.

- Dependent on old, unpatched operating systems and libraries.
- Demonstrated by FDA Safety Alerts issued for vulnerable networked devices.

Need techniques that show how security can be done.

Typical Embedded Device (any domain)

"Brilliant Spaghetti" is not a compliment.

- This is pervasive in many industries and domains.
- We can't get rid of `gets`, do you think we can get rid of 1000 line functions?
- Change is therefore tremendously expensive.
  - Which limits innovation.
  - As well as patches.

Architecture and design often take a back seat to functionality.

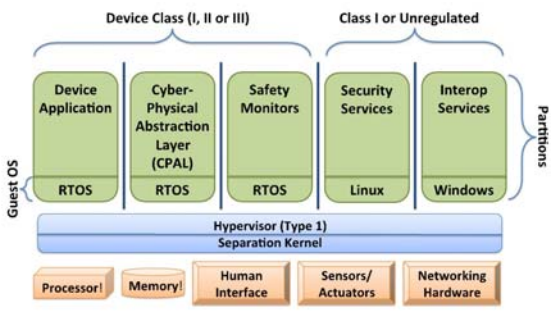
The Talent Gap Limits Progress

- Cybersecurity flaws can lead to patient harm and/or data breach.
  - Regulators want evidence that security has been designed in.
  - Absence of evidence will delay approval and increase time to market.
- Manufacturers have limited resources:
  - Often lack the resources or knowledge to build security in from scratch.
  - The devices still provide **significant** clinical benefits.
- Expert embedded systems security developers are rare and expensive:
  - Often lack safety expertise.
  - Not the same as IT security.

ISOSCELES will provide tools, templates, and services to help systems developers create safe and secure devices.

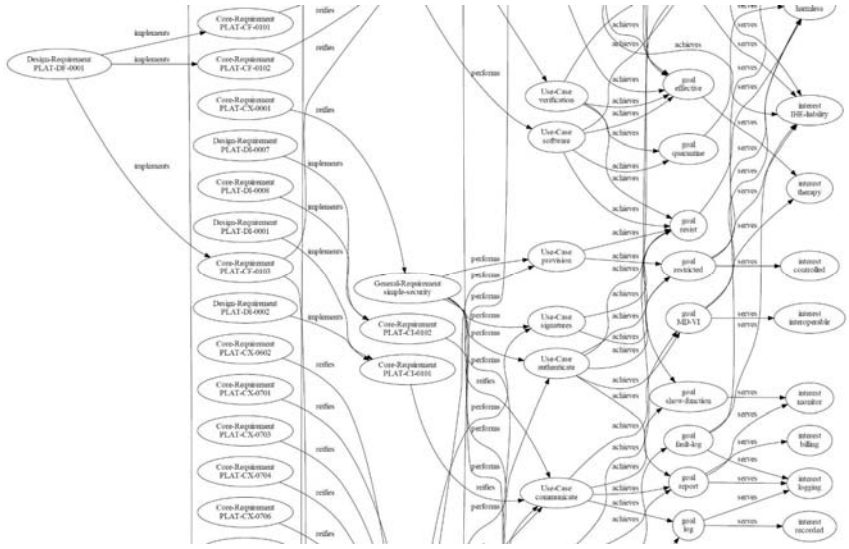
ISOSCELES Approach

- Develop model-driven, configurable medical device platform.
- Separate safety and security functions from the medical application.
- Auto-generate device internal communications and processing directly from the models.



Separation provides many of the desired benefits.

The Challenge Starts with Requirements



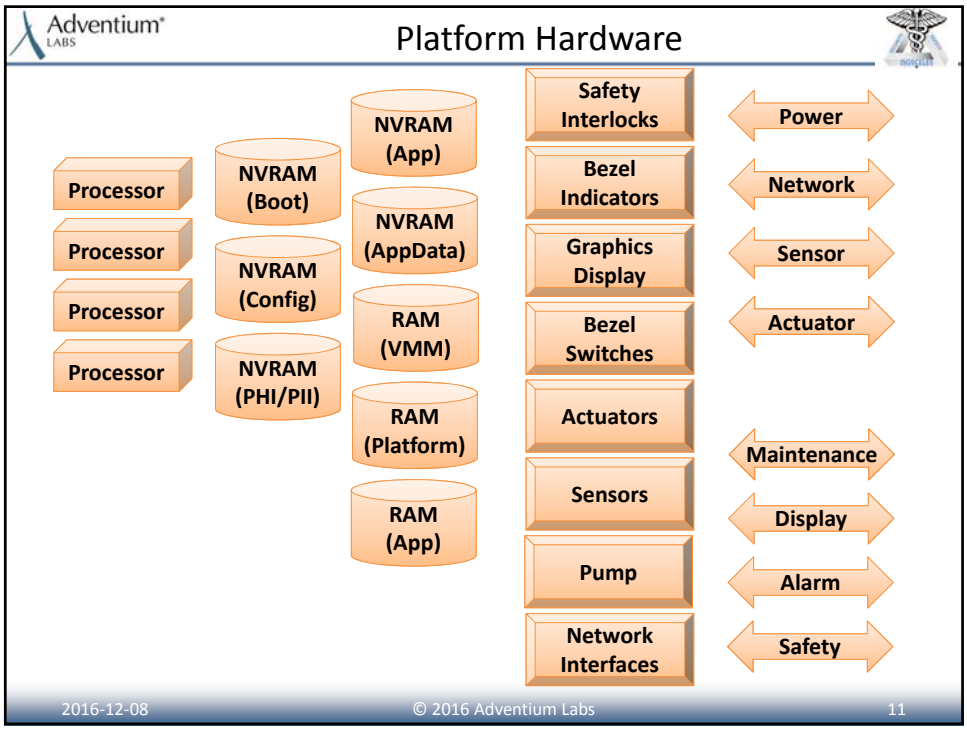
We are using an infusion pump as an exemplar.

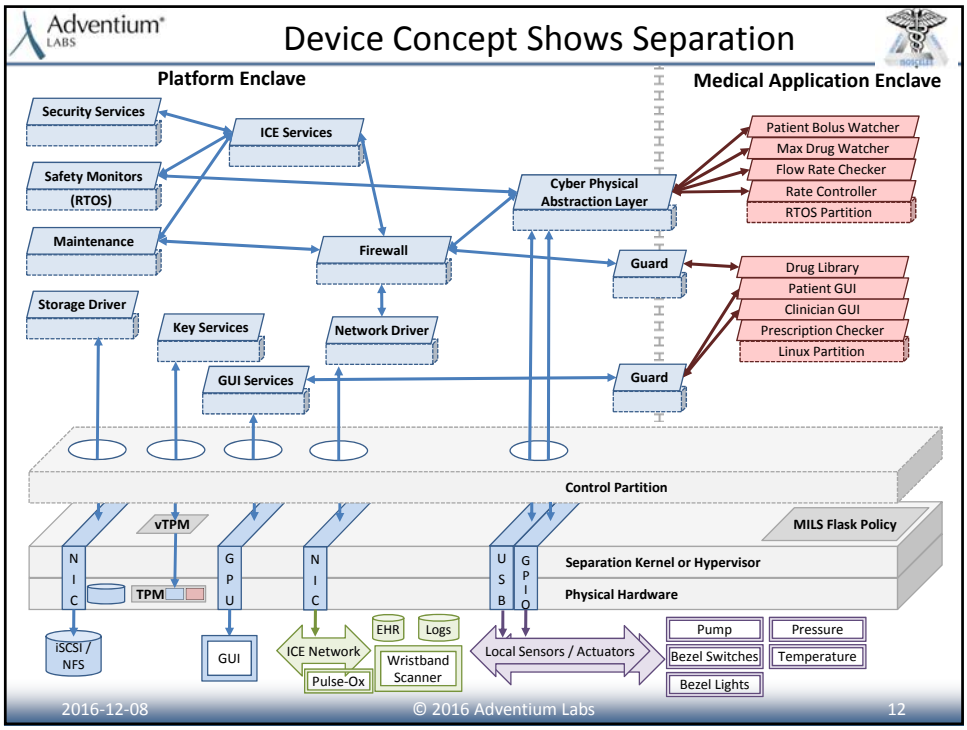
Model-based Systems Engineering (MBSE)

```
public
with common,isosceles;

system demo_sys
end demo_sys;

system implementation demo_sys.impl
   subcomponents
      clinic_wifi: bus common::wifi.impl;
      external_log_host: abstract common::external.log_host;
      external_user_interface: abstract
            common::external.user_interface;
      isosceles_demo: system isosceles::demo.phl;
   connections
      ext_sys: bus access isosceles_demo.ext_network <->
            clinic_wifi;
      ext_log: bus access external_log_host.net <-> clinic_wifi;
      ext_gui: bus access external_user_interface.net <->
            clinic_wifi;
end demo_sys.impl;

end isosceles_phl_demo;
```

- Design is captured in AADL models.
- We will automatically generate platform configuration data from the model:
  - Partition configuration
  - Network configuration
    - Connectivity
    - Separation / firewall rules
  - Safety monitor configuration
  - Module APIs

AADL models will drive system configuration.


Adventium LABS
Platform Hardware
Processor
Processor
Processor
Processor
NVRAM (Boot)
NVRAM (Config)
NVRAM (PHI/PII)
NVRAM (App)
NVRAM (AppData)
RAM (VMM)
RAM (Platform)
RAM (App)
Safety Interlocks
Bezel Indicators
Graphics Display
Bezel Switches
Actuators
Sensors
Pump
Network Interfaces
Power
Network
Sensor
Actuator
Maintenance
Display
Alarm
Safety
2016-12-08
© 2016 Adventium Labs
11


Adventium LABS
Device Concept Shows Separation
Platform Enclave
Medical Application Enclave
Security Services
ICE Services
Safety Monitors (RTOS)
Maintenance
Storage Driver
Key Services
Firewall
Network Driver
GUI Services
Cyber Physical Abstraction Layer
Guard
Guard
Patient Bolus Watcher
Max Drug Watcher
Flow Rate Checker
Rate Controller
RTOS Partition
Drug Library
Patient GUI
Clinician GUI
Prescription Checker
Linux Partition
Control Partition
vTPM
MILS Flask Policy
NIC
TPM
GPU
NIC
USB
GPIO
Separation Kernel or Hypervisor
Physical Hardware
iSCSI / NFS
GUI
ICE Network
Pulse-Ox
EHR
Logs
Wristband Scanner
Local Sensors / Actuators
Pump
Pressure
Bezel Switches
Temperature
Bezel Lights
2016-12-08
© 2016 Adventium Labs
12

Safety Monitors

- Defined safety architecture:
  - separates monitors from what they monitor.
  - With ability to override behavior when unsafe conditions are detected.
- Defined monitor/ response grammar.
  - Triggers
  - Notifications
  - Actions
  - Logging
- ISOSCELES architecture provides:
  - Data connections to monitor partition explicitly declared.
  - Trigger conditions are evaluated at specified frequency.
  - Both local and remote notifications are initiated.
  - Response actions are taken.
  - Safety events are logged for analysis.

Bringing avionics to medicine…

Security Architecture & Services

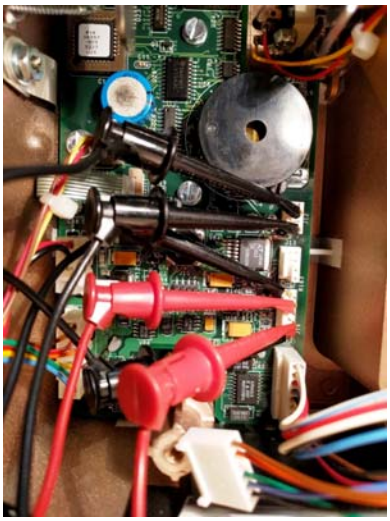
- Partition interactions restricted to those specified in the model.
- Control partition not accessible from network.
- Configurable network firewall.
- Library of additional security controls (e.g. authentication, FIPS cryptography).
- Provisioning mechanisms.
- Secure update mechanisms.
- Analytical evaluation of MBSE artifacts.
  - E.g. Analyze to verify that PHI data is not being written to a network device logs.
  - Verify real-time performance requirements are satisfied.

MBSE will help control development process.

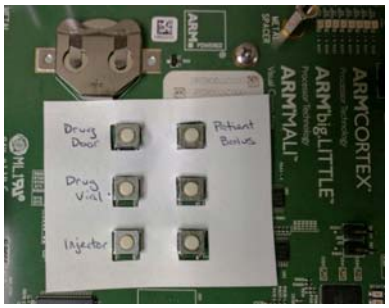
Separation Layer

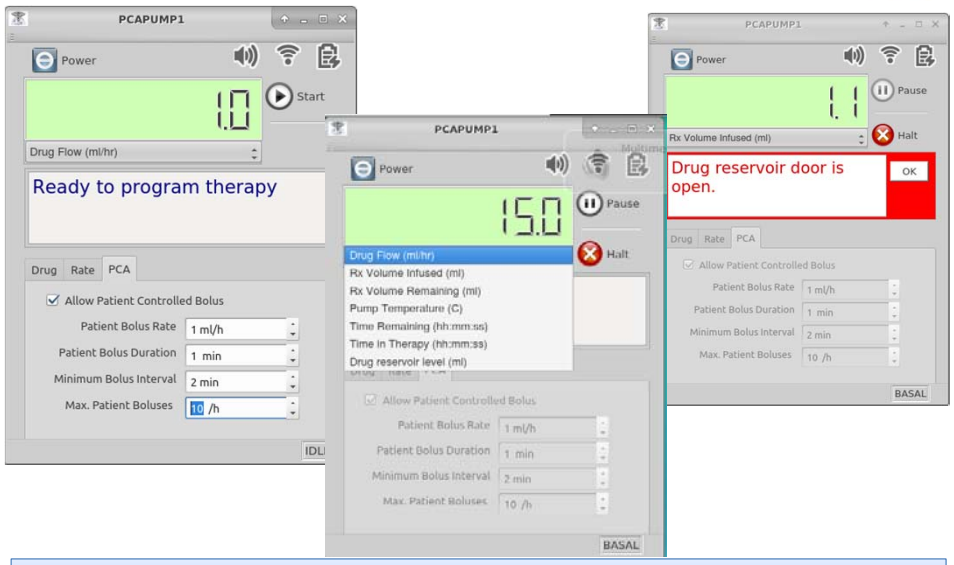
- For Phase 1 – We are using Xen for prototyping.
- We have full demo running on Ubuntu 16.04 on Xen 4.6 on small iEi G-Series x86 board.
- We will select target separation approach early 2017.
  - Balance provable separation, cost, and features.
  - Embedded support may be a sticking-point.
- We want platform flexibility
  - Difference choices may be appropriate for different device targets.
- Goal is to extract AADL info into an intermediate form that can be easily targeted to alternate separation layers and/or hypervisors.
  - We will implement the back end for our chosen target.

Inside Parts



Phase I Functional Demo





Start like a regular company: Functionality

ISOSCELES Benefits

Reduce cost of development and operations:

- Meet market needs without having dedicated security experts in-house.
- Provides the architecture and models to address documentation expected by the FDA.
- Quicker time to market.
- Lower risks of having to deploy many security patches.
- When patches are needed, there are lower regulatory hurdles due to strong partitioning.

This will allow users to jump-start core competencies.

Possible Alternate Approaches

- Hiring in-house security expertise.
- Contract hardware/software design to a custom design house.
- Do nothing (aka “Faith-based risk management”)
- Or use a configurable platform.
  - We are not aware of similar capabilities in the medical device space.

Safety and security must be included from the start.

Summary

- Medical device security is desperately needed and is becoming expected.
- ISOSCELES will provide
  - Tools and templates for the small company.
  - Examples and techniques that can be incorporated by large companies.
- We are currently wrapping up MBSE and requirements.
- We plan to build initial configuration tooling, the target platform, and create a more complete PCA-pump exemplar.

We intend to open-source the platform.

Future Efforts

- Data input protocols.
- Network communications protocols.
- User Interface human factors.
- Implantables.
- Remote updates.
- Country-specific privacy controls.

- *Control authority during abnormal situations.*

We still need solutions for many basic areas.

