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

AADL Committee Meeting
2017-06-07
Todd Carpenter, Chief Engineer, Adventium Labs
Dr. John Hatcliff, Kansas State University
Dr. Kevin Fu, University of Michigan

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.

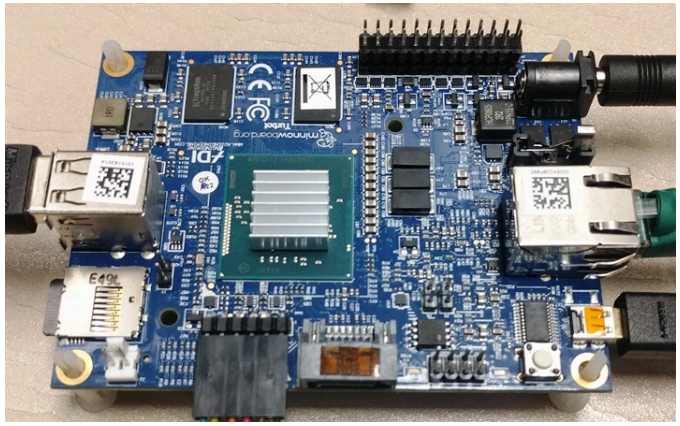
Executive Summary

Need:

- Inadequate security of many networked medical devices can lead to *unacceptable risk* to patients, clinics, and businesses.
- The lack of evidence of good security designs will delay FDA approval.

Approach:

- We are developing a partitioned safe and secure medical device platform.
- Medical device companies can build their medical application on this platform.
- ISOSCELES will produce open-source *education*, *requirements*, *model-based designs*, and *example HW & SW implementations*.



Benefits:

- Shorter time-to-market for safe and secure devices.
- Fewer security issues with fielded devices.
- Easier updates when patches are necessary.

Competition:

- Attempt to apply IT security to medical devices.
- Pay someone else to do it, with no way of determining quality of results.
- Rely on testing, check-lists, and compliance-based approaches.

ISOSCELES will spur safe and secure innovation.

ISOSCELES Team

US Department of Homeland Security Project, CPS Security Program, $2.2million for 3 years

Adventium Labs

- Todd Carpenter (PI) – Safety and security critical systems including avionics, industrial control, medical devices, and weapons systems.
- Dr. Steve Harp – safety and security critical systems, architecture design.
- Jim Carciofini – safety critical system design and engineering, model based systems engineering.
- Steve Johnston – embedded systems development.
- John Gohde – software engineering, security.

Kansas State University:

Information and Telecommunications Technology Center

- Dr. John Hatcliff (PI) – Safety critical model-based medical device design.
- Dr. Eugene Vasserman – Medical device security.
- Brian Larson – PCA pump, model based systems engineering.

University of Michigan:

Security and Privacy Research Group

- Dr. Kevin Fu – Medical device security evaluation.

Medical Device Industry Needs

80% of device manufacturers have 50 or fewer employees.

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

- Companies focus on therapy and diagnostic innovations.
- Start-ups rarely have the resources to build in security from scratch.

Small companies need tools and templates.

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

- Devices depend on old, unpatched operating systems and libraries.
- FDA Safety Alerts have been issued for vulnerable networked devices.

Large companies need appropriate security solutions.

Developer Needs

- Expert embedded systems security developers are rare and expensive.
- IT security experts often lack experience with:
  - Constrained embedded systems.
  - Safety, integrity, and availability.
  - Quality systems, including formal requirements and design.
- MedCo quality systems focus on safety.
  - Not set up for business risks.
  - Difficult for developers to motivate non-safety related security.

Most Top Computer Science Programs Skip Cybersecurity

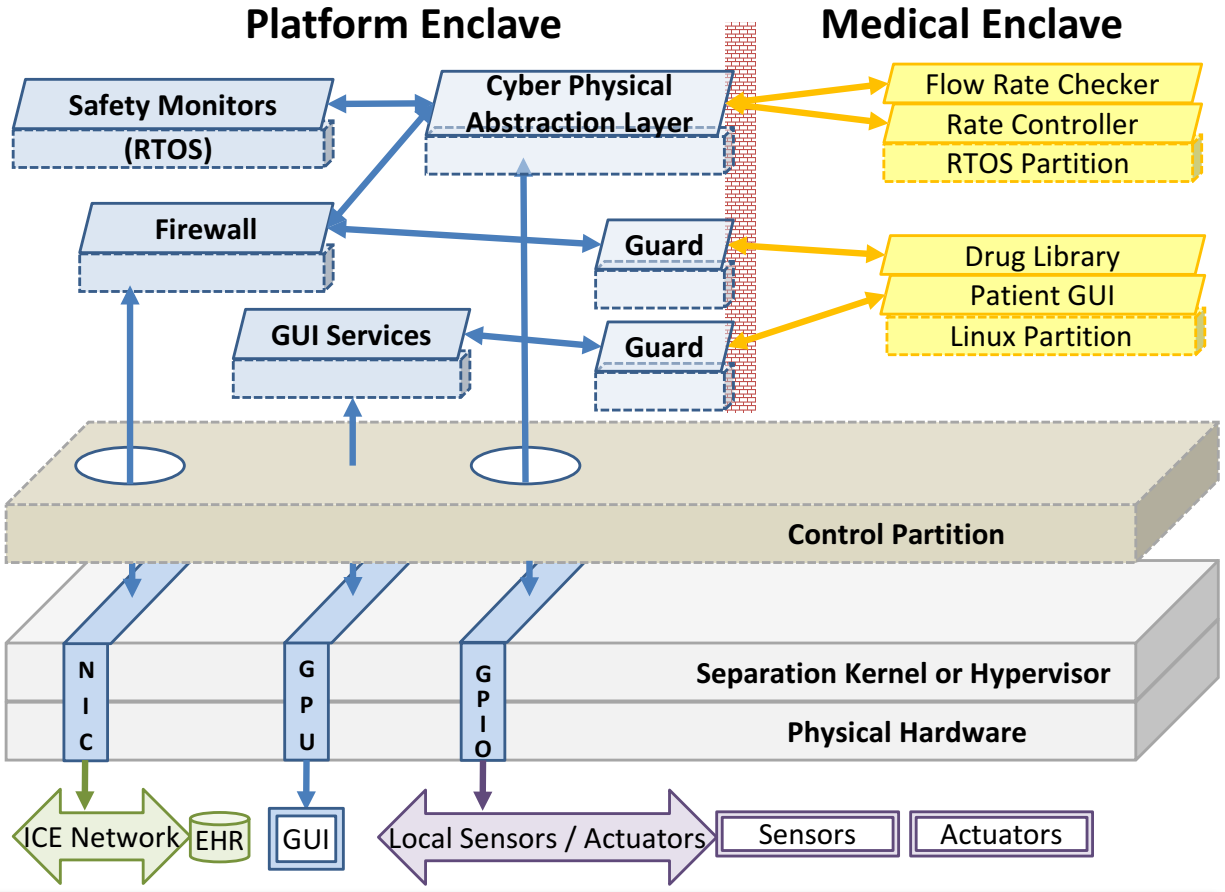
- Only three of the top 50 university computer science programs in the United States require students to take a cybersecurity course.
- Many don't even offer a class on the subject.
- Graduates of computer science and engineering programs are not qualified to fill cybersecurity positions.
- 200,000 US cybersecurity job openings are unfilled

http://theinstitute.ieee.org/career-and-education/education/most-top-computer-science-programs-skip-cybersecurity

Developers need a foundation to build upon.

ISOSCELES Model Driven Separation Approach

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



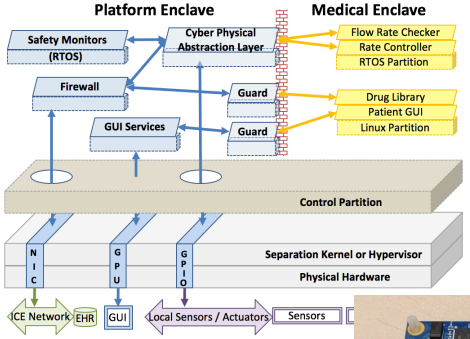
Architecture separates networking from safety functions.

ISOSCELES Product-Line Engineering Approach

ISOSCELES-based Medical Devices

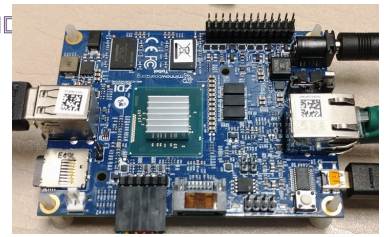
(note: concept illustrated – pictured devices not built using ISOSCELES)

ISOSCELES platform assets are instantiated/configured to develop devices for specific care-giving functions



Hypervisors / Micro-kernels

- Zen
- SeL4
- …

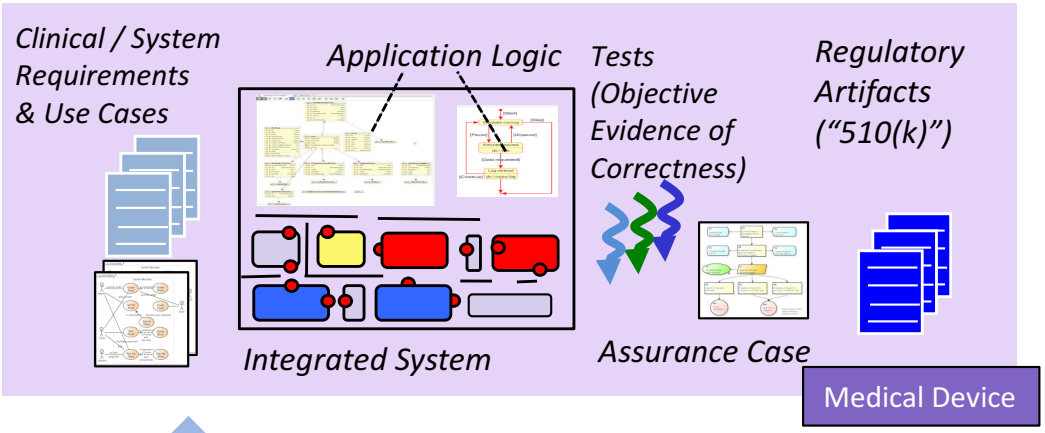


Safety/Security Services

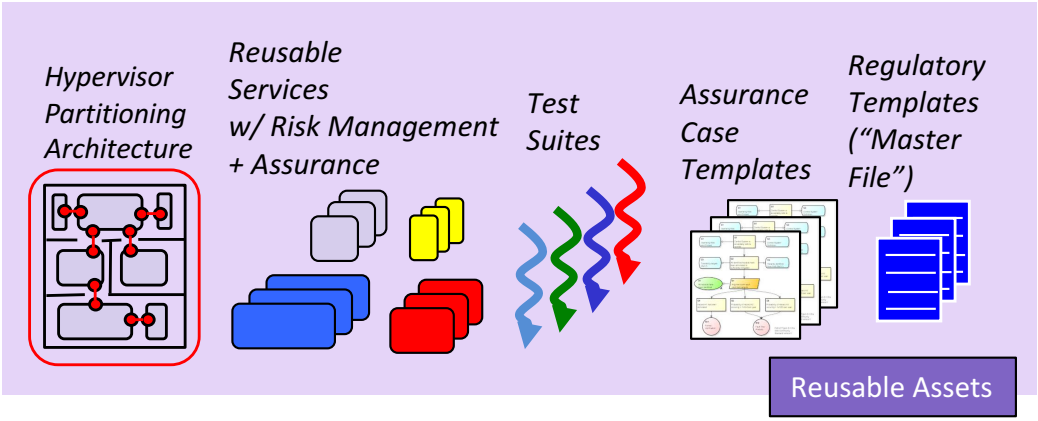
- Process Partitioning
- Communication Partition
- Encryption
- Authentication
- Logging
- Etc.

ISOSCELES Platform Assets

Application Engineering



Systems Engineering process for instantiating platform assets

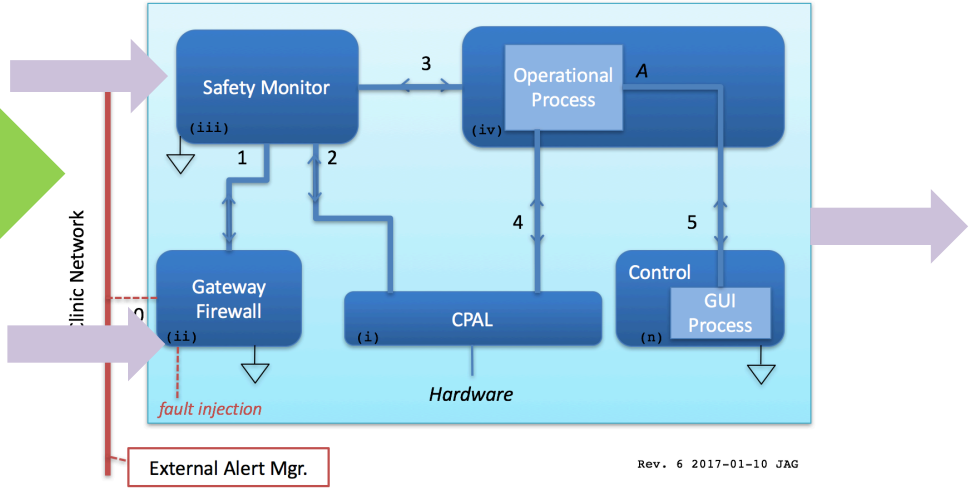


Domain/Platform Engineering

From Spaghetti to Partitioned Architecture

Typical Embedded Device

Strongly Partitioned Function/Communication



Use of ISOSCELES model-driven hypervisor technology to achieve strong partitioning in runtime architecture

Benefits to Stakeholders

- Separate networking, safety, and security functions from the medical application
- Fault isolation
- Easier / better handling of updates (updating only relevant partitions) and reassurance
- Etc.

Patient-Controlled Analgesic (PCA) Pump

PCA Pump Background

- PCA Pump is used to pump an analgesic drug (opioids, pain-killers) into a patient's intravenous infusion (IV) line to provide pain relief
- The infusion is "patient controlled" because the patient presses a button to release a dose of the drug. The "burst of drug" released when the button is pressed is called a "bolus dose"

PCA Pump on ISOSCELES

- FDA created "Infusion Pump Improvement Initiative" due to safety concerns for pumps.
  https://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202501.htm
- ISOSCELES will develop a prototype infusion pump using the ISOSCELES platform
- PCA Pump device selected because
  - KSU previously developed extensive pump artifacts w/ FDA engineers in **NSF FDA Scholar-in-Residence Program**
  - PCA example is widely used in current standards development for interoperable systems

ISOSCELES Development – Primary Elements

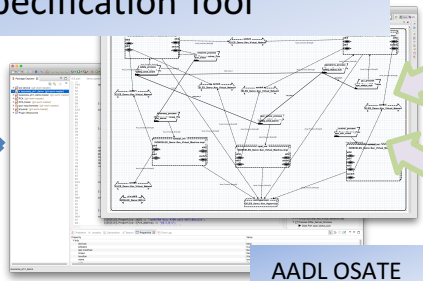
Medical Device Requirements

Risk Management (Safety, Security Analysis)

Assurance Cases V & V Evidence

Regulatory Artifacts

ISOSCELES Architecture Specification Tool



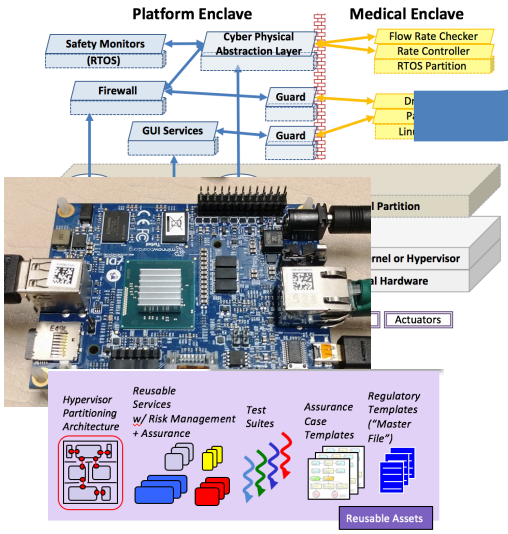
AADL OSATE

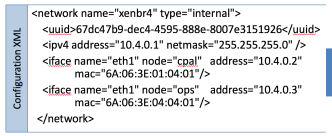
Medical Device Software

Medical Device-specific Hardware (sensors, actuators)

ISOSCELES platform configuration and device development is organized in a **model-centric** development process.

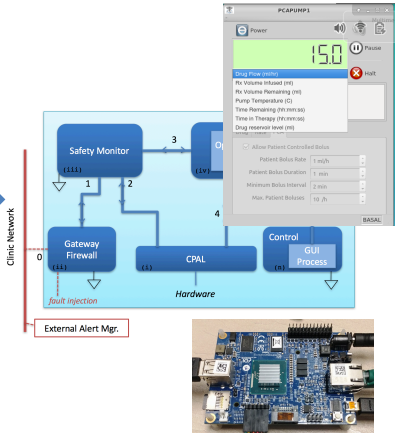
ISOSCELES Platform Assets





ISOSCELES Platform Configuration (XML)

ISOSCELES Platform Deployment & Configuration Framework

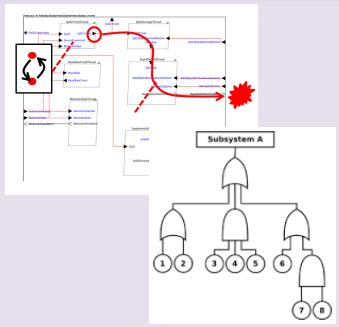


ISOSCELES Platform Run-Time Environment

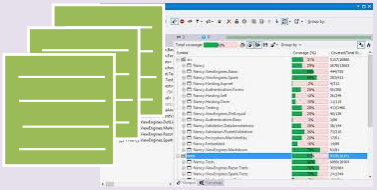
ISOSCELES Stakeholder Artifacts

ISOSCELES focuses not only on software/hardware, but also addresses **artifacts** necessary to help manufacturers integrate ISOSCELES into their development context, align with relevant standards, and support regulatory submissions.

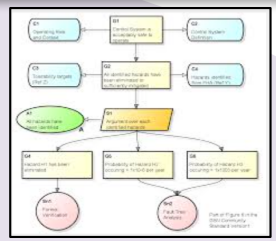
Risk Management (Safety/Security Hazard Analysis)



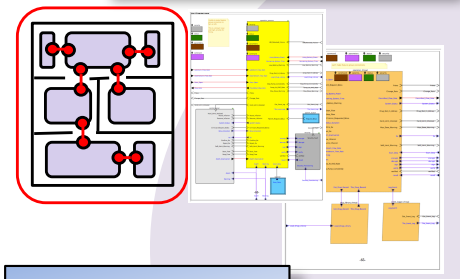
V & V artifacts (test suites/ reports)



Assurance Cases



Architecture Models (design)



Standards Compliance

Underwriters Laboratories

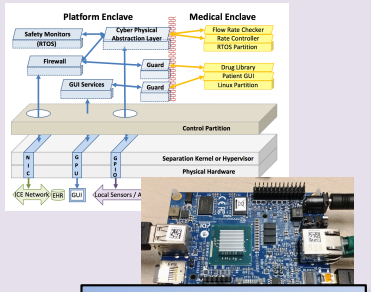
AAMI
Advancing Safety in Healthcare Technology

ISO IEC

Requirements

Regulatory Submission Artifacts

US Food & Drug Administration
FDA
APPROVED

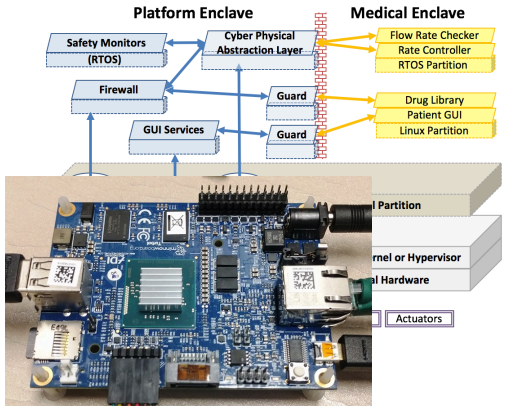


Hardware & Software

Constellation of artifacts necessary for using software/hardware assets in regulated industry context

Modeling Platform Assets [Demo OSATE]

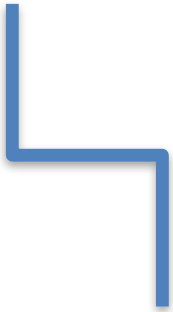
ISOSCELES Platform Assets



Hypervisor Building Blocks

Partitions / Virtual Machines

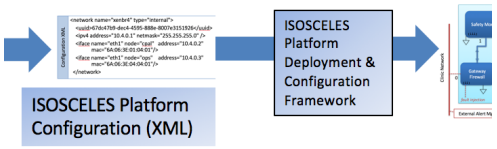
Virtual Networks



Hypervisor Building Blocks Properties

- General
  - UUID, etc.
- VM
  - OS
  - Memory
- Networking
  - IP Address
  - IP Network Mask
  - MAC Address
- Logical Communication
  - Protocols
  - QoS

Reminder: Tool Chain Pipeline



When the ISOSCELES deployment and configuration framework encounters instances of these modeling building blocks in the XML-based configuration info, it will do the appropriate instantiation/implementation in the "build" of the platform instance.

ISOSCELES Safety/Security Services

- Firewall
- Network Guards
- Authentication
- Encryption
- Logging
- …

Medical Device Domain Building Blocks

- Medical Domain Information Schema
- Physiological Data Representations
- GUI Services
- Sensor/Actuator Driver wrappers
- …

Model-based Systems Engineering (MBSE)

- Capture separation design in AADL.
- Analyze the models to provide evidence, e.g., of separation, performance.
- This reduces test burden.
- ISOSCELES will then automatically configure the platform:
  - Partition configuration.
  - Network connectivity, separation, firewall rules.
  - Safety monitors.
  - Module APIs.

AADL

```
connections
  cpal_status_1: port cpal_server_process.cpal_status_pub ->
                 operations_process.cpal_status_sub {
    Actual_Connection_Binding => (reference (xenbr4));  };
  cpal_status_2: port cpal_server_process.cpal_status_pub ->
                 safety_process.cpal_status_sub {
    Actual_Connection_Binding => (reference (xenbr2));  };
```

Configuration XML

```
<pubsub_channel name="cpal_status">
  <port name="CPAL_PUBPORT" protocol="TCP">5001</port>
   <publisher node="cpal" process="cpal-server" address="*"/>
   <subscriber node="ops" process="operations"
address="10.4.0.3"/>
   <subscriber node="safety" process="safety"
address="10.2.0.7"/>  </pubsub_channel>
```

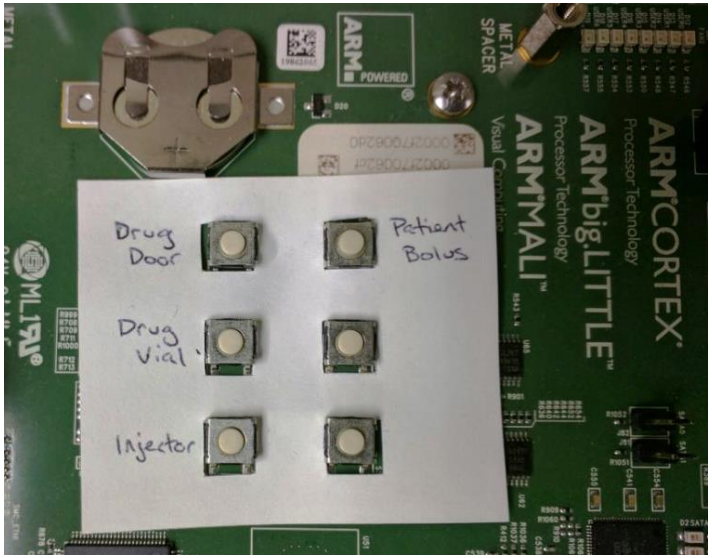
AADL models will drive system configuration.

Separation Layer

- Open source Xen hypervisor provides separation in initial prototype.
- Software demonstration runs on AMD G-series SoC, Intel Atom prototyping boards, and PCs.
- We will select and mature one separation approach in 2017.
  - Balance provable separation, cost, and features.
  - Mature embedded systems support is an issue.
- We want platform flexibility; one size does not fit all.
- We will extract information from AADL into an intermediate form that we can target to different separation layers.

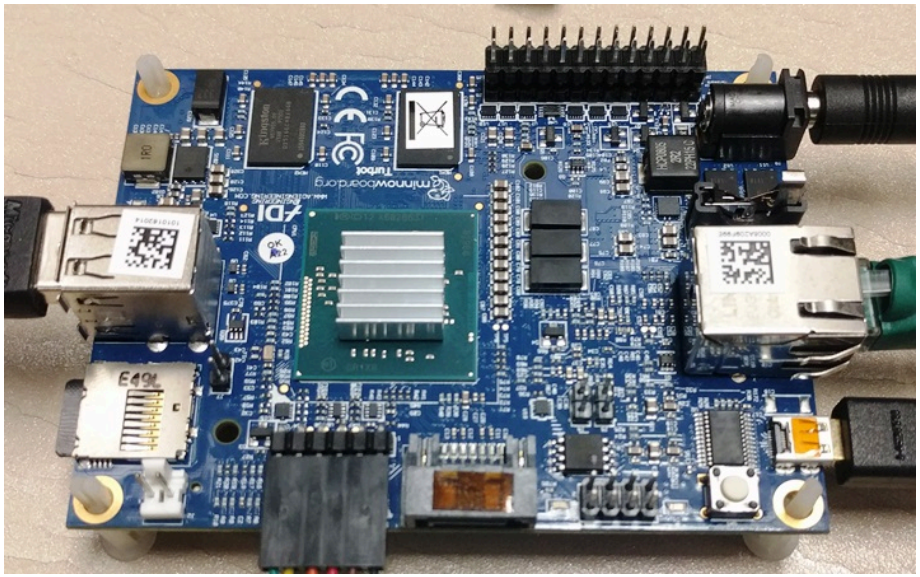
Current focus is on the Xen hypervisor and SeL4.

Prototype Hardware



Current boards:

- ARM v7 Arndale, Tegra TK1 (seL4)
- ARM v8 Juno (Linux)
- AMD x64 iEi G-series (Xen)
- Intel ATOM Minnowboard (Xen)



Multiple targets and environments will reduce adoption costs.

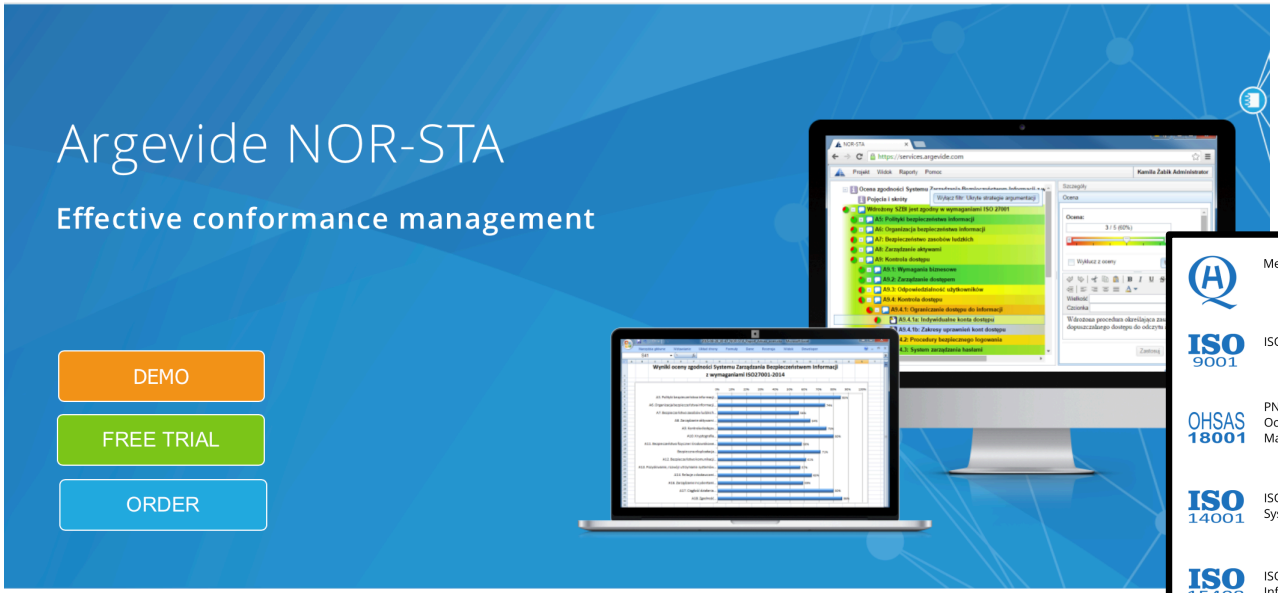
Conclusions

- Demo Goals:
  - Illustrate our initial use of hypervisor technology (from point of view of both platform manufacturer and device manufacturer)
  - Illustrate model-based development methodology and workflow
- Next Steps
  - Further vetting demo concept with device industry partners and FDA collaborators
  - Investigating additional hypervisors/micro-kernels in the context of end-to-end development
  - Adding realism and greater configurability to both the platform and PCA device elements

EXTRA SLIDES

Industrial Integration – Assurance Artifacts

Argevide produces the **NOR-STA assurance case tool** used in a number of safety-critical domains by industrial clients throughout Europe.



Standards targeted by NOR-STA with built-in support.

	Medical Standards	ISO 27001	ISO 27001 Information Security Management
ISO 9001	ISO 9001 Quality management systems	IEC 62443	IEC 62443 Security for industrial automation and control systems
OHSAS 18001	PN-N 18001 / OHSAS 18001 / ISO 18001 Occupational Health and Safety Management	ISO 26262	ISO 26262 Road vehicles – Functional safety
ISO 14001	ISO 14001 Environmental Management Systems	IEC 61511	EN/IEC 61511: Functional safety – Safety instrumented systems for the process industry sector
ISO 15408	ISO/IEC 15408 Common Criteria for Information Security Evaluation	ISO 17065	ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services
HACCP	HACCP Hazard Analysis and Critical Control Points	caf	Common Assessment Framework CAF 2006 and CAF 2013

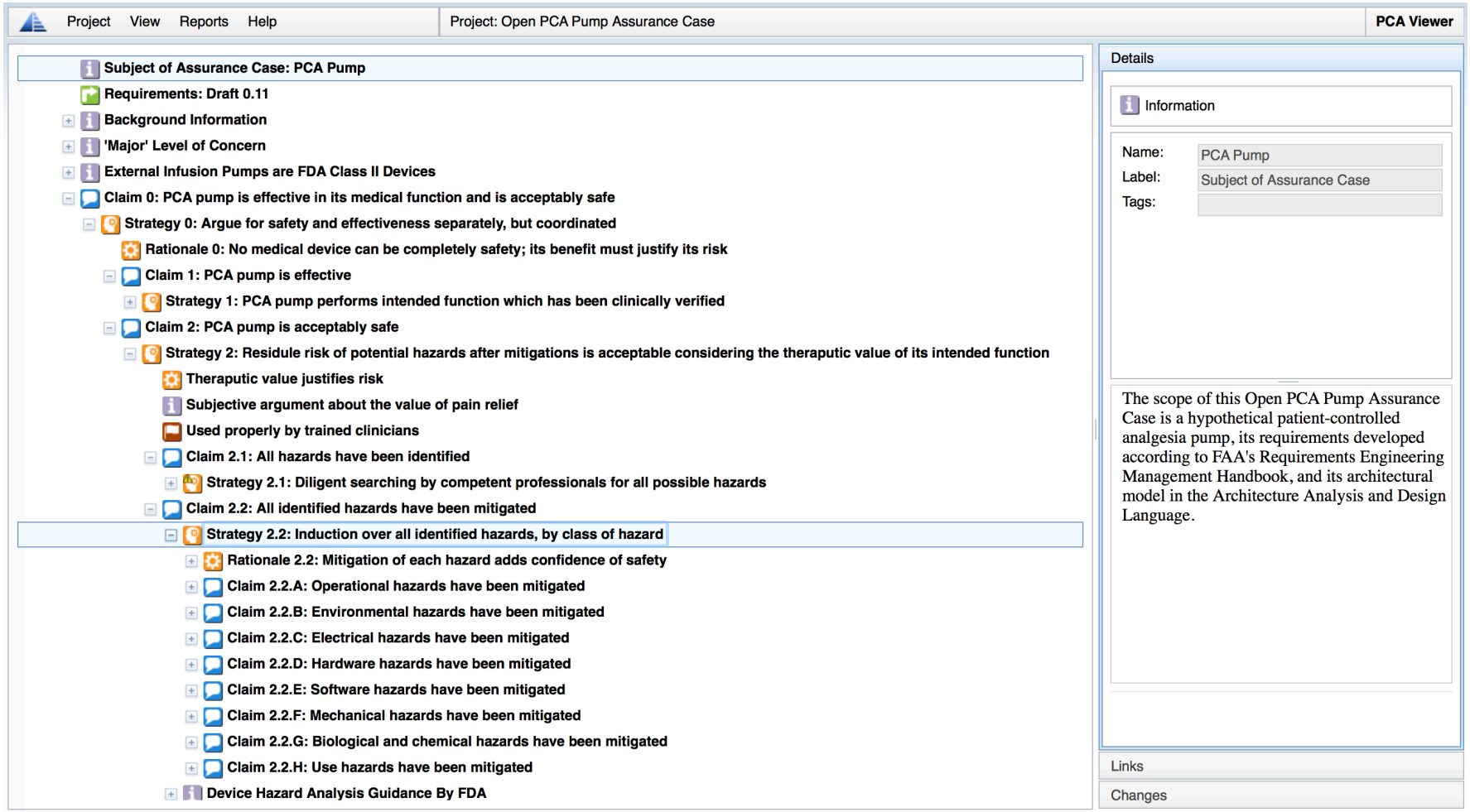
- KSU worked with Argevide to get FDA funding to develop an assurance case template to be used in regulatory submissions to FDA.
- Now working with Argevide and FDA to develop templates and examples for safety/security assurance cases for interoperable medical devices – aligned with assurance structures used in AAMI/UL 2800

https://www.argevide.com

Industrial Integration – Assurance Artifacts

Preliminary version of ISOSCELES PCA Pump Assurance Case in NOR-STA tools

(DEMO: walk-through NOR-STA web-interface for pump assurance case)



Industrial Integration – Assurance Artifacts

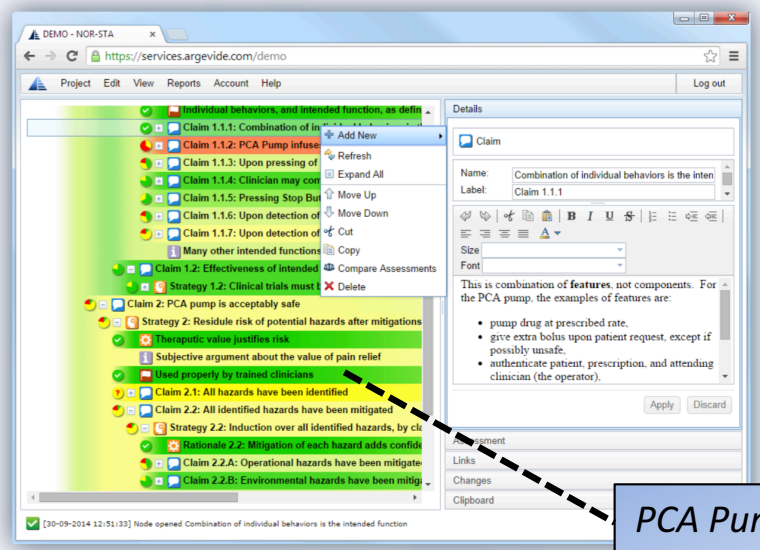
PCA Pump Assurance case originally developed under NSF FDA Scholar-in-Residence funding and now being extended on ISOSCELES is used by NOR-STA as one of the canonical examples in their training material

ARGEVIDE

www.argevide.com

Argevide NOR-STA features

- You can **develop** and **manage** large and complex argument structures.
- Tree view in NOR-STA facilitaties **browsing large arguments**.
- You can easily **copy and paste** fragments of the argument.
- You may use various options of **report generation.**
- NOR-STA is compliant with **ISO/IEC 15026** requirements.
- You can use OMG **ARM/SACM** import and export functions. Any ARM/SACM project can be easily imported to NOR-STA.
- When needed NOR-STA can generate **GSN** diagrams for your reports.



PCA Pump Assurance Case develop by KSU used in NOR-STA training

https://www.argevide.com/wp-content/uploads/2016/05/Argevide-NOR-STA-assurance-case.pdf

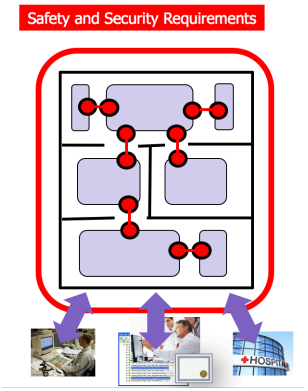
Alignment with Emerging Safety/Security Standards

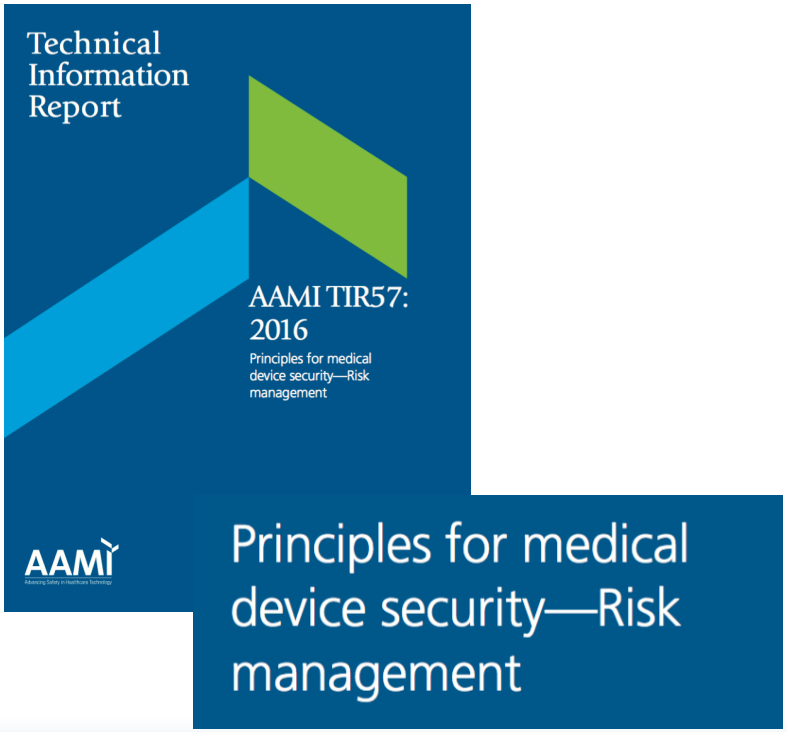
Cross-fertilization and deep integration with medical device safety/security standards that ISOSCELES team members and their close associates are involved in

- AAMI/UL 2800 family of safety/security standards for interoperable medical systems
  - Architecture, life-cycle processes, risk management (somewhat analogous to ISO 26262)
  - emphasis on ***platform-based engineering***
  - ISOSCELES team member Hatcliff is co-chair of primary working group; Vasserman leads security subgroup
  - ***Primary working example in 2800 support material is PCA Pump use case***
- AAMI TIR 57: Principles for medical device security – Risk Management
  - AAMI Security Group co-chair by Ken Hoyme from Boston Scientific (formally ISOSCELES PI from Adventium Labs)
- NIST Security Standards

AAMI
Advancing Safety in Healthcare Technology

Underwriters Laboratories





ISOSCELES Work Force Training Resources

The following indicates some of the support material posted on course/project web page to provide background information to students/researchers

PCA Pump in nutshell

- Patient Controlled Analgesia (PCA) Pumps: The Basics

PCA Clinical Tutorials from Columbia Gorge Community College

- PCA Introduction (http://www.youtube.com/watch?v=RAI5sPOAxqU)
- PCA Setup I (http://www.youtube.com/watch?v=RtWjHQN-wu8)
- PCA Setup II (http://www.youtube.com/watch?v=kXaMW754Hk4)
- PCA Initiation (http://www.youtube.com/watch?v=GDIoo___tkg)
- PCA Manage I (http://www.youtube.com/watch?v=GMbYHvgfY2U)
- PCA Manage II (http://www.youtube.com/watch?v=eYPrtxHG5e8)

Training videos for prep'ing and operating PCA Pump in a clinical context

Baxter PCA Pump Tutorial

- http://www.youtube.com/watch?v=KqGCOLIgIqE

PCA Clinical Guidelines

- *Patient-Controlled Analgesia: Making it Safer for Patients* , Cohen et al. (.pdf)
- *Patient-Controlled Analgesia: Guidelines of Care*, San Diego Patient Safety Taskforce (.pdf)
- *Acute Post operative Analgesia Guidelines: Patient Controlled Analgesia*, Royal Cornwall Hospitals, UK (.pdf)
- *Patient Controlled Analgesia (PCA) Policy for Adult and Paediatric Patients*, West Hertfordshire, UK (.pdf)

Industry/Clinical safety guidelines for PCA management

PCA Pump Prescription Forms and Drug Dosage

- Physician's Order Form -- New Hanover Regional Medical Center (.pdf)
- Physician's Order Form -- Overlake Hospital Medical Center (.pdf)
- Physician's Order Form -- St. Luke's Hospital (Chesterfield, MO) (.pdf)
- Morphine Dosage

Physician Order Forms for PCA Infusion

PCA Pump Prescription Auto-Programming

- *From Smart Pumps to Intelligent Infusion Systems – The Promise of Interoperability*, Patient Safety and Quality Health Care, May/June 2014. (.pdf)

PCA Pump Product Spec Sheets and Marketing Materials

- ambBIT ambulatory pump from Summit Medical Products, Inc. (marketing spec sheet, product web site)
- Alaris SE Pump (user manual, technical service manual)
- CADD-Prizm Ambulatory Infusion Pump (general description, clinician information, technical manual)

Example PCA Pump product operating and service manuals

PCA Pump Problems

- Mary E. Burkhardt's keynote presentation at the conference "Improving Medication Safety Through Effective Communication and Teamwork." (http://www.youtube.com/watch?v=wY3YyyQjvtQ)
- Paolo Masci's presentation on user interface oddities and problems in infusion pumps. (https://www.youtube.com/watch?v=T0QmUe0bwL8)

Improving Pump Safety via Monitoring of Respiratory Health

- A story about a loss of life and motivation for dedicated monitoring for PCA pumps using capnography (http://www.youtube.com/watch?v=gNZbvs3aByc)
- Medical Device Plug-n-Play Project's overview of using the Integrated Clinical Environment (ICE) to implement a safety-interlock for a PCA pump based on capnography and pulse oximetry monitoring. (http://www.mdpnp.org/MD_PnP_Program___Clinical_S.html) (see the videos under Scenario #1)
- Clinical study on PCA monitoring -- Maddox et al. "Continuous Respiratory Monitoring and a `Smart' Infusion System Improve Safety of Patient-Controlled Analgesia in the Postoperative Period." (.pdf)
- Clinical study on PCA monitoring -- Maddox et al. "Clinical Experience with Capnography Monitoring for PCA Patients." (.pdf)
- Clinical study on PCA monitoring -- Overdyk et al. "Improving Outcomes in Med-Surg Patients with Opiod-Induced Respiratory Depression." (.pdf)

Clinical studies on PCA safety issues

http://openpcapump.santoslab.org/node/1