Medical Application Platforms – Rationale, Architectural Principles, and Certification Challenges

http://people.cis.ksu.edu/~hatcliff/Medical-Application-Platforms.pdf

Contact: hatcliff@ksu.edu, http://people.cis.ksu.edu/~hatcliff/

John Hatcliff
Kansas State University

Andrew King, Insup Lee
University of Pennsylvania

Alasdair MacDonald
eHealth Technology

Anura Fernando
UL (Underwriters Laboratories)

Michael Robkin
Anakena Solutions

Eugene Vasserman
Kansas State University

Sandy Weininger
US Food and Drug Administration

Julian M. Goldman
Massachusetts General Hospital
CIMIT MD PnP Program

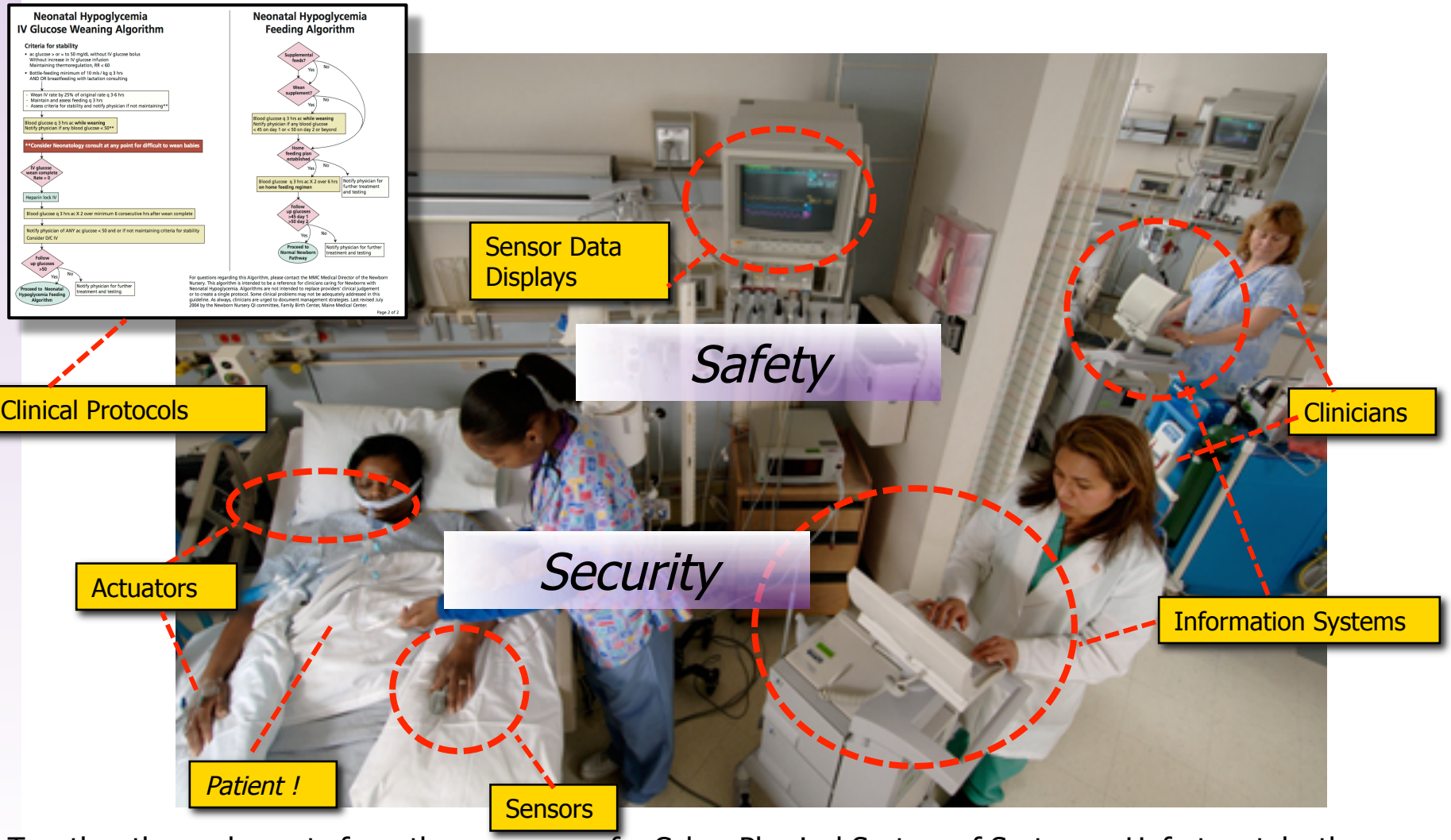
Acknowledgements/Collaborators:

MD PnP Project led by Dr. Julian Goldman at CIMIT
NIBIB Quantum Health Care Intranet Team
Medical Device Coordination Framework (MDCF) Teams at KSU and U Penn
AAMI / UL 2800 Committee Members

Support:

Funding provided by US National Science Foundation awards 0734204, 0930647, 0932289, 1065887, 1239543, 1355778 (Cyber-Physical Systems and FDA Scholar-in-Residence programs) and the NIH/NIBIB Quantum program

Health Care Involves A Variety of System Components

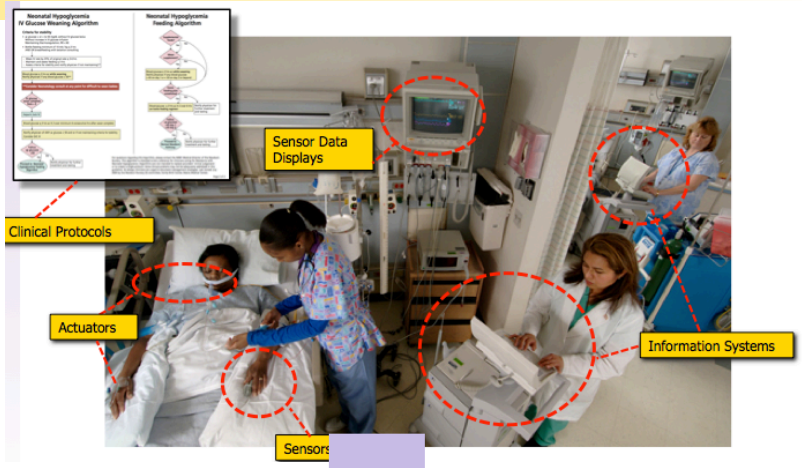


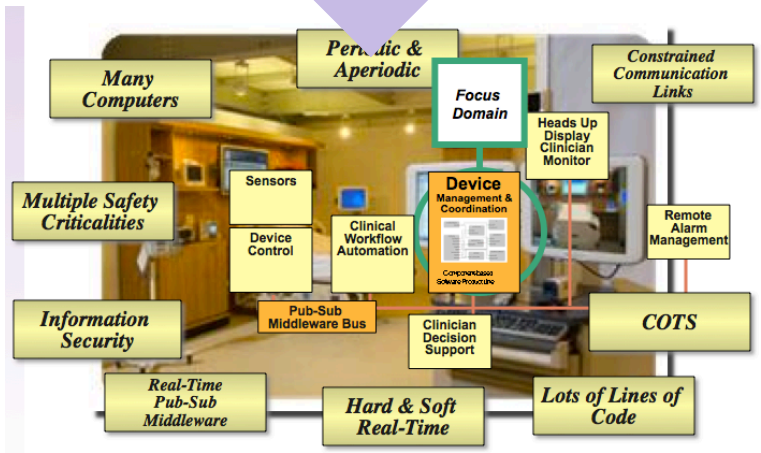
Together these elements form the precursor of a Cyber-Physical System of Systems. Unfortunately, these elements are largely un-integrated, and so appropriate automated systems solutions cannot be applied.

This Talk

High-level presentation of issues related to architecture/regulation – not specific solutions

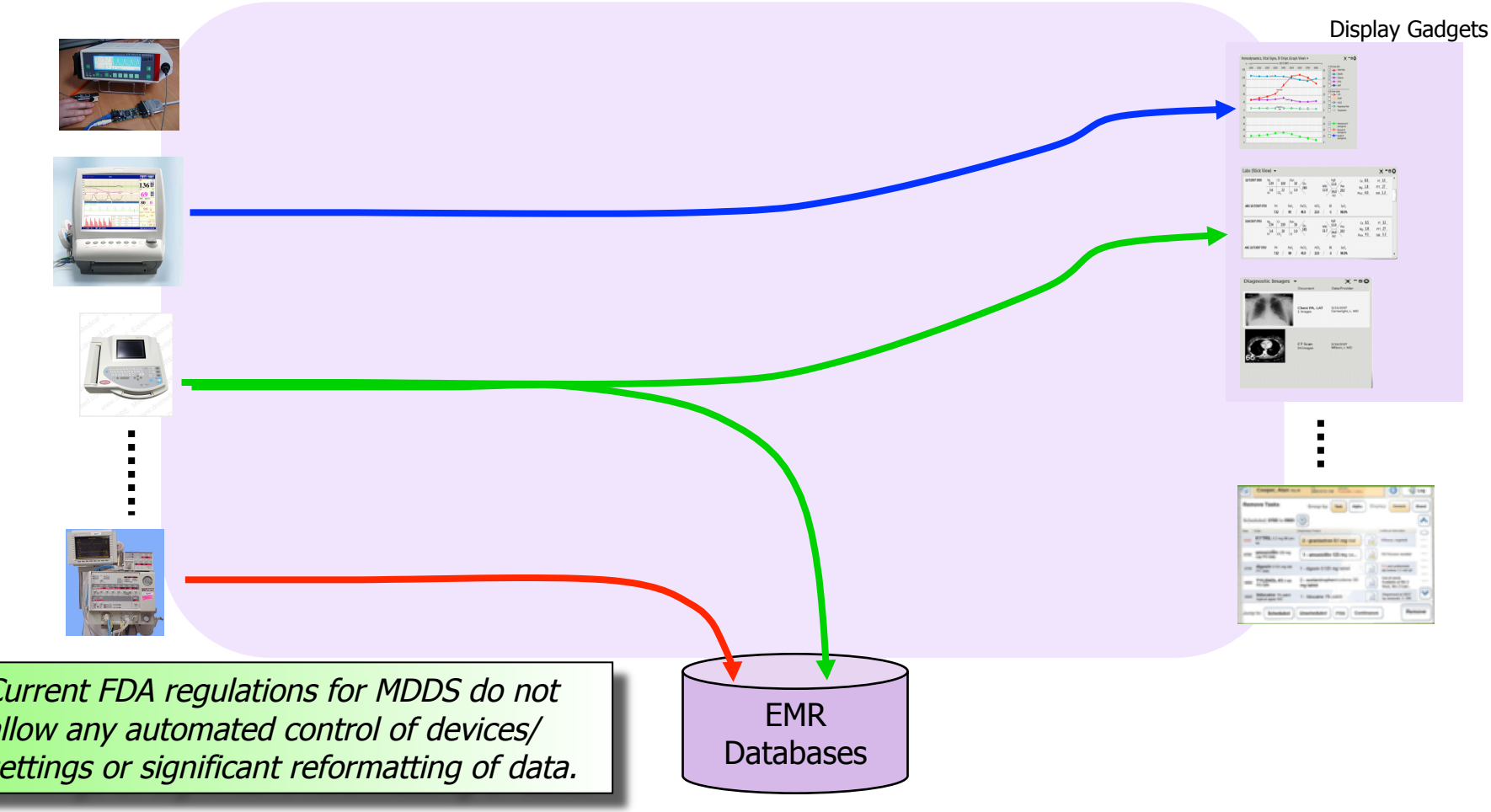
- Clinical motivation for cyber-physical systems of systems
  - See also talks from Dr. Julian Goldman
- Concept of a Medical Application Platform (MAP)
- Distinguishing characteristics of MAPs
- Integrated Clinical Environment – an architectural standard for MAPs
- Interoperability Safety Standards (AAMI / UL 2800)





Recent Commercial Systems

Medical Device Data Systems (MDDS) -- Data only flows from producers to consumers; data must be faithfully re-presented



Current FDA regulations for MDDS do not allow any automated control of devices/ settings or significant reformatting of data.

Integrating Data Streams

Fully leverage device data streams

Devices

***Moving forward**: aggregating data streams to create "smart alarms" that reduce nuisance alarms by triggering alarms only when multiple physiological parameters are in agreement, e.g., agreement in trends on ET CO2 as well as pulse ox SpO2*

Data Consumers

iAware Gadgets

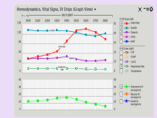
Data Stream 1

Data Stream 2

Smart Alarm Logic

Alarm Info

"Medical Device Integration Platform application (app)"



Nurse Station

Sensor fusion

From Wikipedia, the free encyclopedia

Sensor fusion is the combining of sensory data or data derived from sensory data from disparate sources such that the resulting information is in some sense *better* than would be possible when these sources were used individually. The

Why is it so hard to do this in the health care space?

Safety Interlocks

Fully leverage device data streams and the ability to *control* devices

***Moving forward**: aggregating data streams to solve **systems problems** by making devices context aware.*

Devices

O_2 Conc. Data

Laser Activation Data

Laser Disable Command

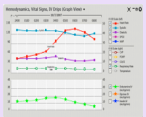
Disable laser if inspired O_2 is > 25%.

Safety Interlock Logic

Alarm Info

Data Consumers

Display Gadgets



Surgical Team

Tracheal tube fire hazard -- caused by failure to reduce O_2 concentration during tracheal laser surgery

Just enforcing a system invariant!

Proposed and published by Sem Lampotang, PhD, Univ. of Florida -- not commercially available. Device coordination systems can provide a solution.

From Dr. Julian Goldman -- MDPnP.

Closed Loop Safety Interlock

Example Use-Case: PCA Monitoring

- Patients are commonly given patient-controlled analgesics after surgery
- Crucial to care, but numerous issues related to safety

A 49-year old woman underwent an uneventful operation (total abdominal hysterectomy and bilateral salpingo-oophorectomy). Postoperatively, the patient complained of severe pain and received intravenous morphine sulfate in small increments. She began receiving a continuous infusion of morphine via a patient controlled analgesia (PCA) pump. A few hours after leaving the PACU [post anethesia care unit] and arriving on the flow, she was found pale with shallow breathing, a faint pulse, and pinpoint pupils. The nursing staff called a "code", and the patient was resuscitated and transferred to the intensive care unit on a respirator. Based on family wishes, life support was withdrawn and the patient died. Review of the case implicated a PCA overdose. Delayed detection of respiratory compromise in patients undergoing PCA therapy is not uncommon because monitoring of respiratory status has been confounded by excessive nuisance alarms.

Simple Closed Loop Control

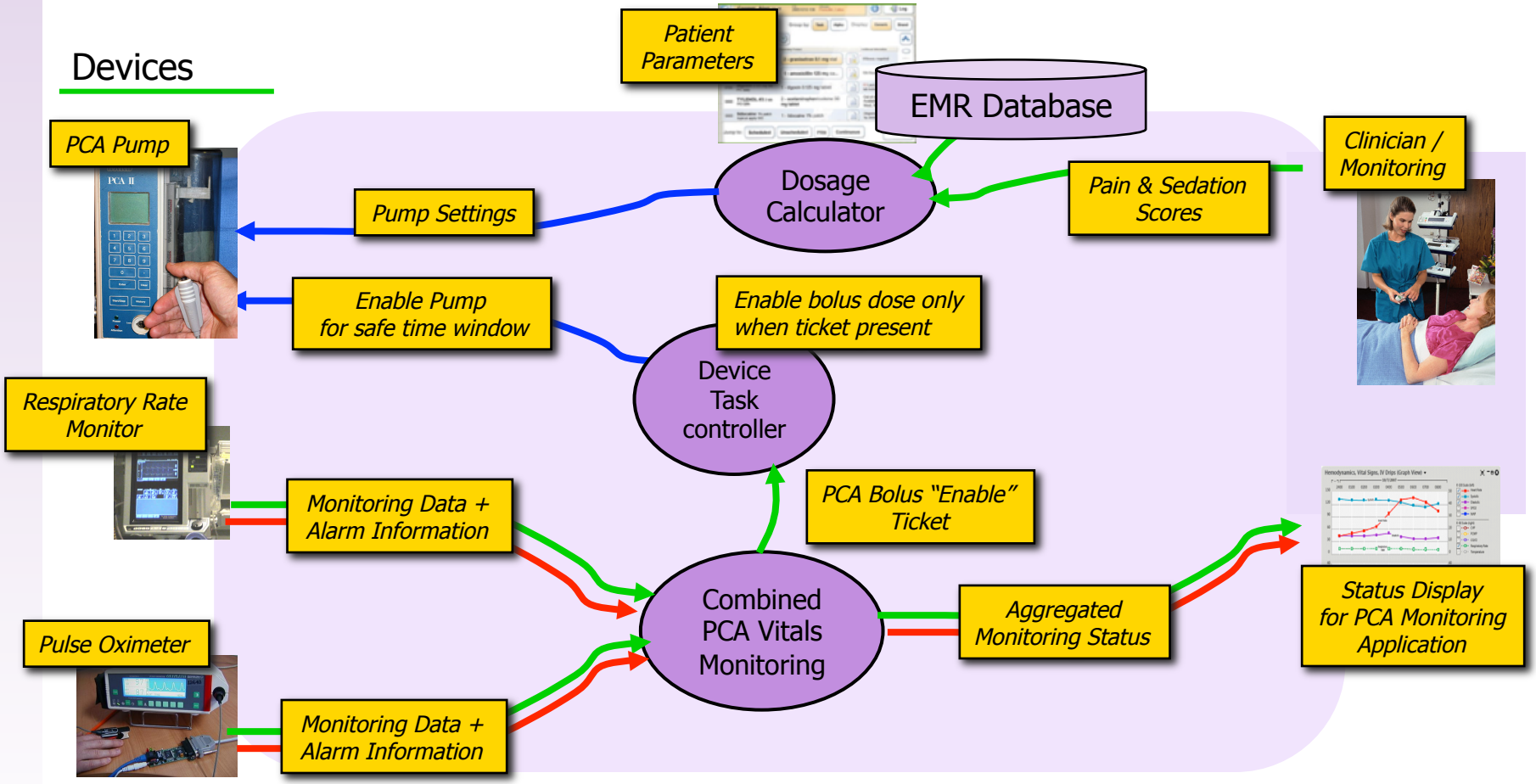
Motivating Clinical Problem: PCA Overdose

apsf
www.apsf.org
NEWSLETTER
The Official Journal of the Anesthesia Patient Safety Foundation
Volume 21, No. 4, 61-88
Circulation 80,350
Winter 2006-2007
Dangers of Postoperative Opioids
APSF Workshop and White Paper Address Prevention of Postoperative Respiratory Complications

- "A particularly attractive feature may be the ability to automatically terminate or reduce PCA (or PCEA) infusions when monitoring technology suggests the presence of opioid-induced respiratory depression. To facilitate such capabilities, we strongly endorse the efforts to develop international standards for device interoperability and device-device communication.
- It is critical that any monitoring system be linked to a reliable process to summon a competent health care professional to the patient's bedside in a timely manner. "

Closed Loop Safety Interlock

Fully leverage device data streams and the ability to *control* devices

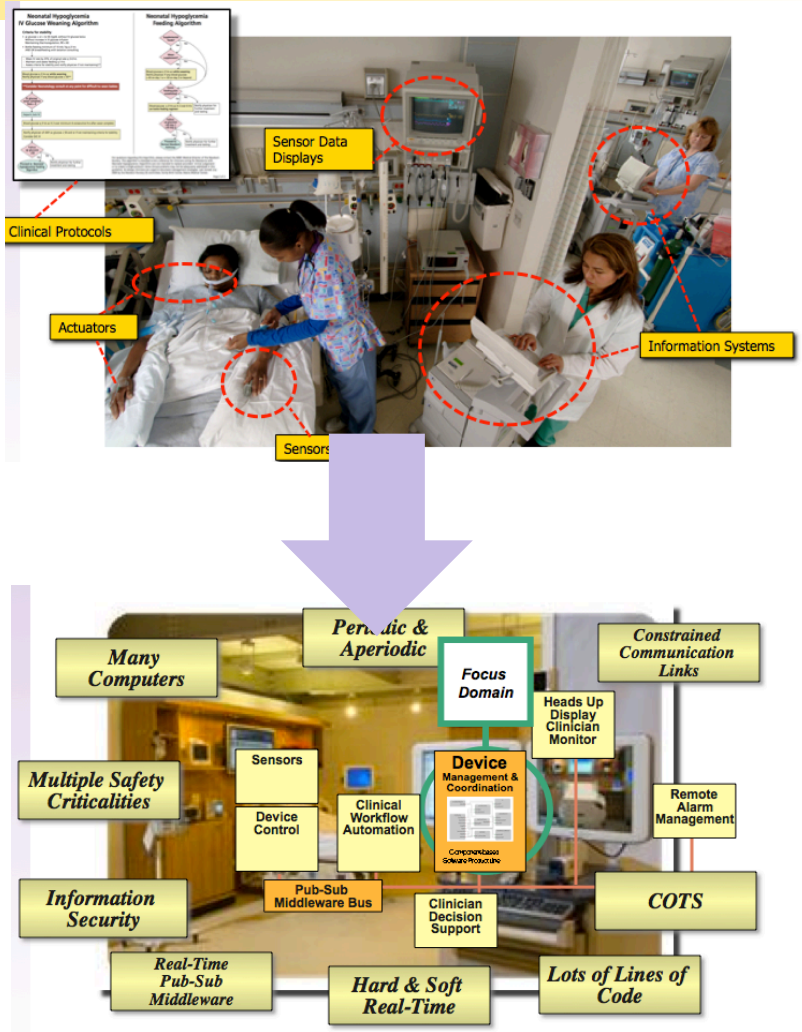


See the paper for a number of other examples, many drawn from the ASTM Integrated Clinical Environment standard.

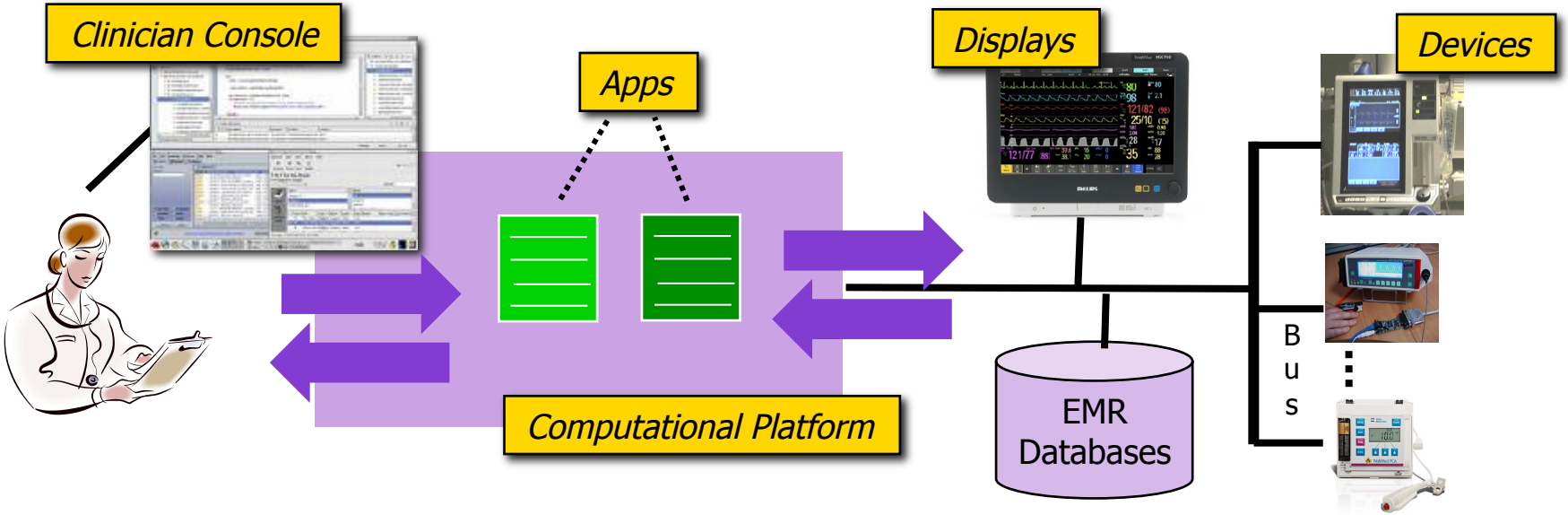
This Talk

High-level presentation of issues related to architecture/regulation – not specific solutions

- Clinical motivation for cyber-physical systems of systems
  - See also talks from Dr. Julian Goldman
- Concept of a Medical Application Platform (MAP)
- Distinguishing characteristics of MAPs
- Integrated Clinical Environment – an architectural standard for MAPs
- Medical Device Coordination Framework (MDCF) – an open source framework for prototyping MAP concepts



Medical Application Platforms

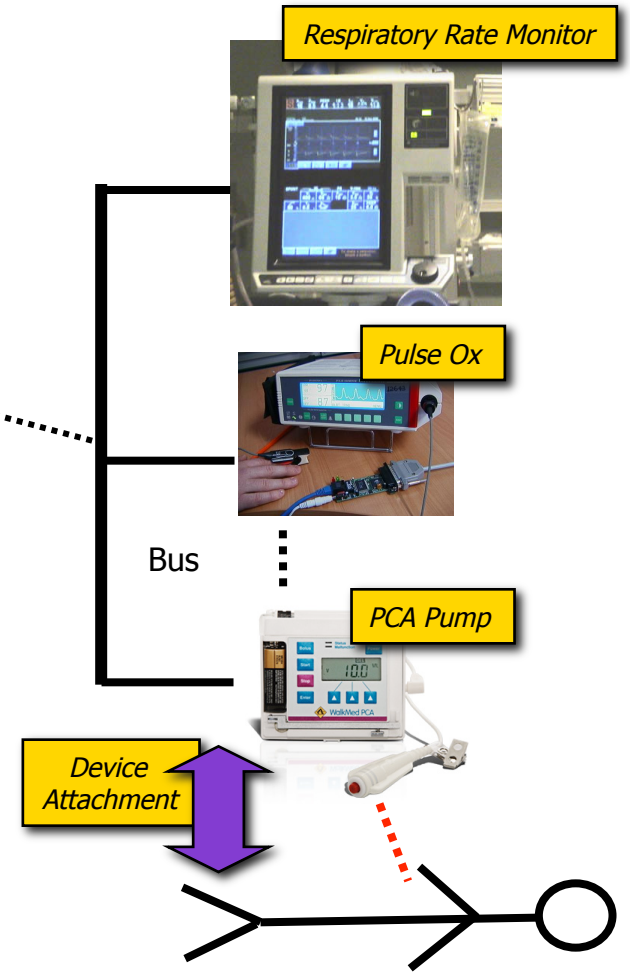


- A *Medical Application Platform* is a safety- and security-critical real-time computing platform for…
  - Integrating heterogeneous devices, medical IT systems, and information displays via communications infrastructure, and
  - Hosting applications ("apps") that provide medical utility via the ability to acquire information from and update/control integrated devices, IT systems, and displays

MAP Functional View

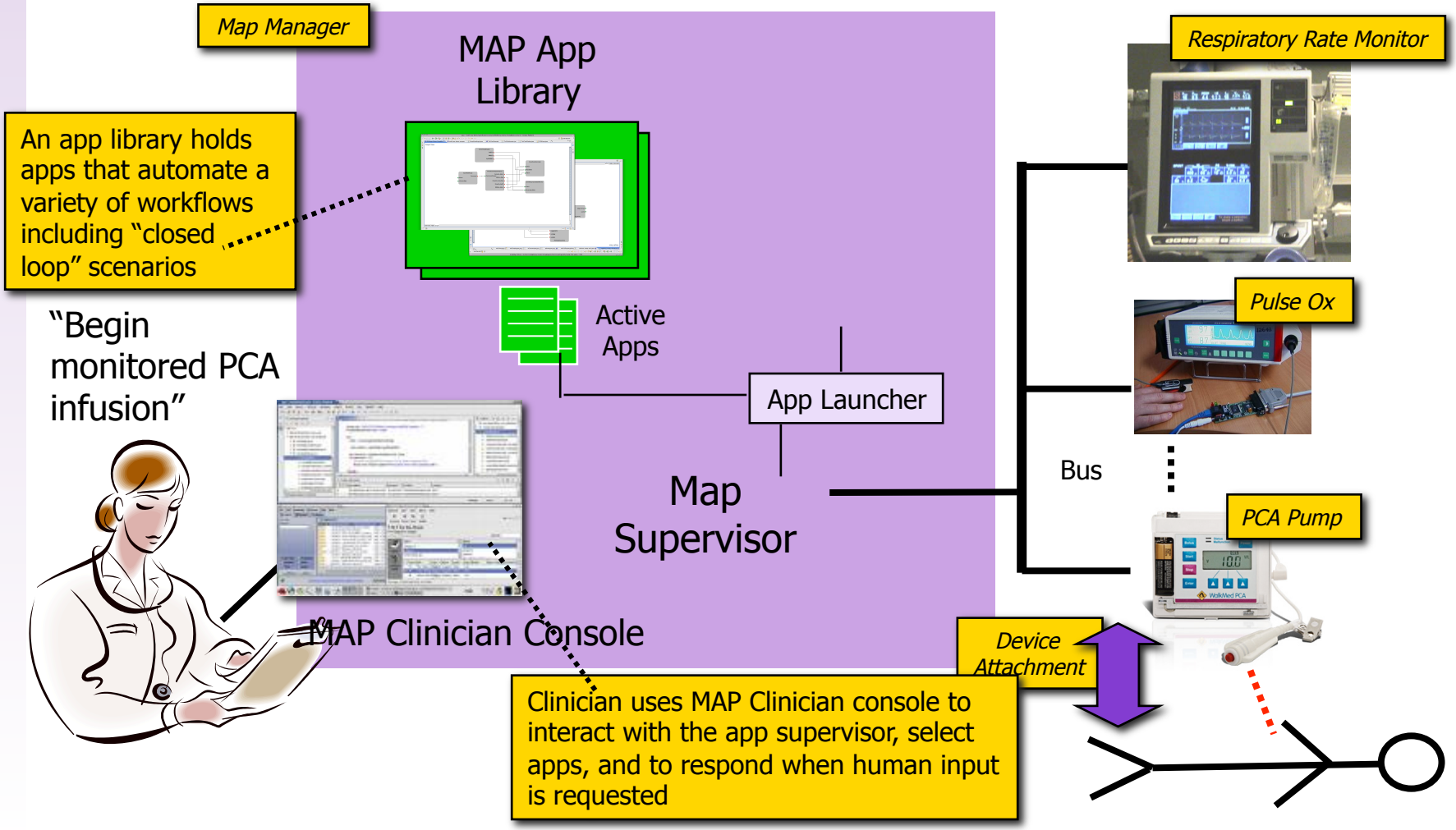
Develop a bus-based app for implementing a safety interlock by coordinating monitoring of vitals with pump control…

Pulse ox, respiratory rate monitor, infusion pump with hand-held control are connected to the patient.



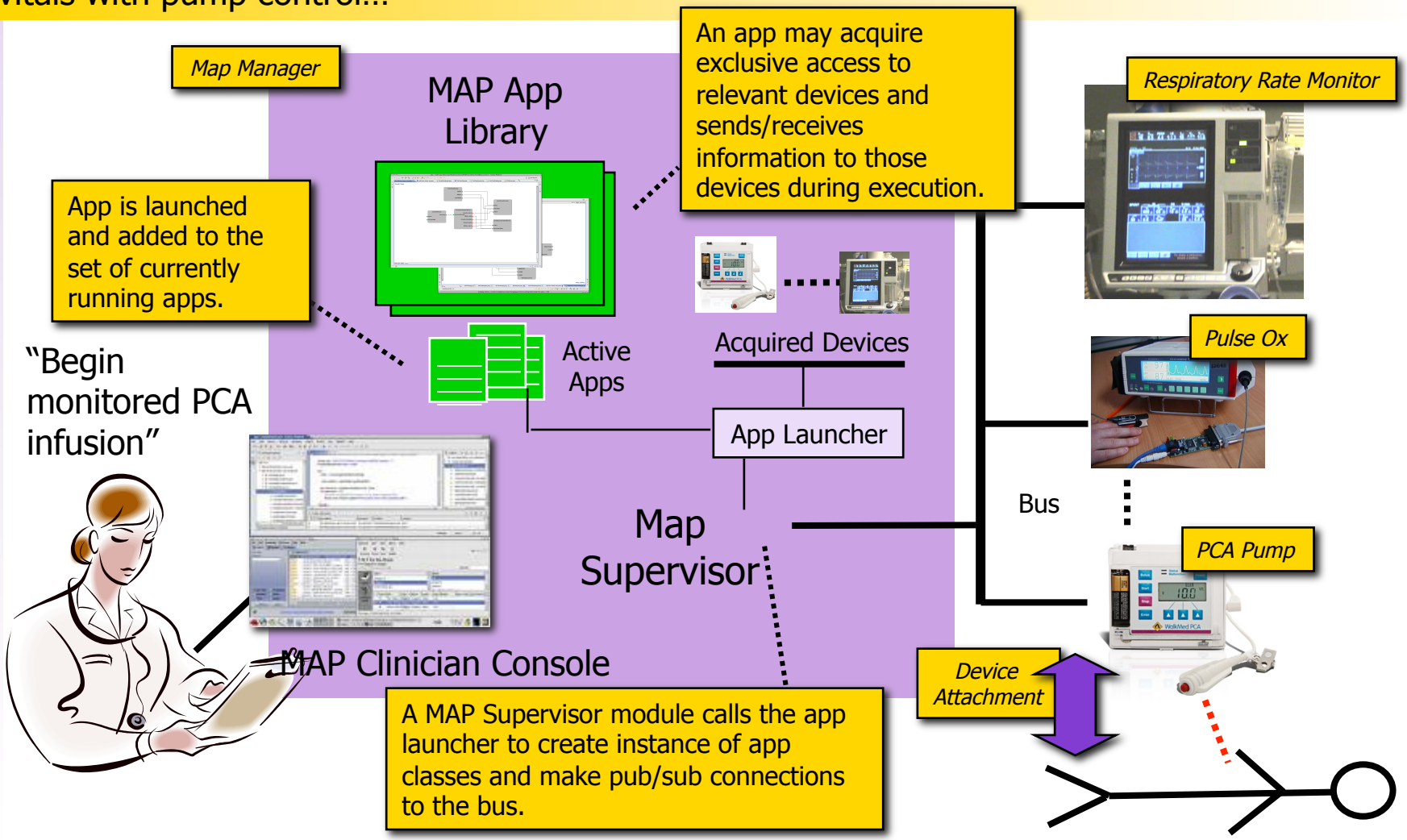
MAP Functional View

Develop a bus-based app for implementing a safety interlock by coordinating monitoring of vitals with pump control…



MAP Functional View

Develop a bus-based app for implementing a safety interlock by coordinating monitoring of vitals with pump control…



Variety of Applications

Apps may provide a variety of clinical functions

- Medical data display and storage
- Derived / Smart alarms
- Clinical decision support
- Workflow automation
- Safety interlocks
- Closed loop control

Link to additional clinical scenario examples

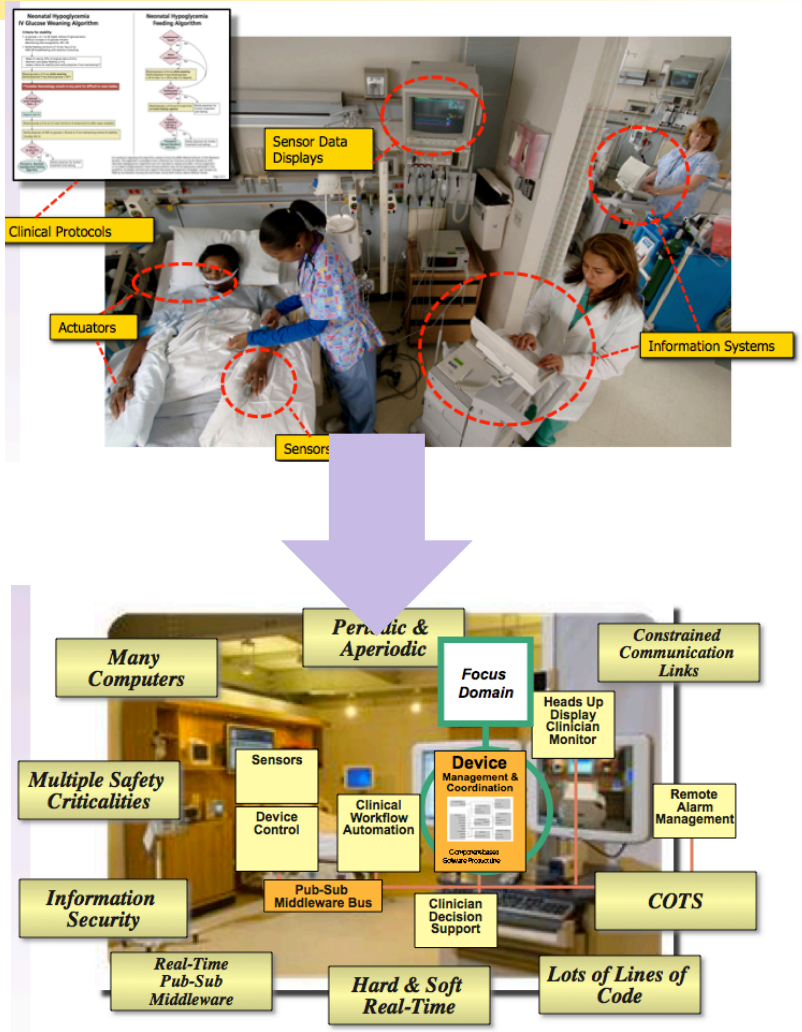
Apps can be categorized according to criticality/risk

- Different degrees of regulatory scrutiny
- Possible determining factors…
  - Intended use
  - Devices read only
  - Devices controlled…
    - Only patient data set
    - Static configuration of monitoring/treatment parameters
    - Dynamic configuration of monitoring/treatment parameters

This Talk

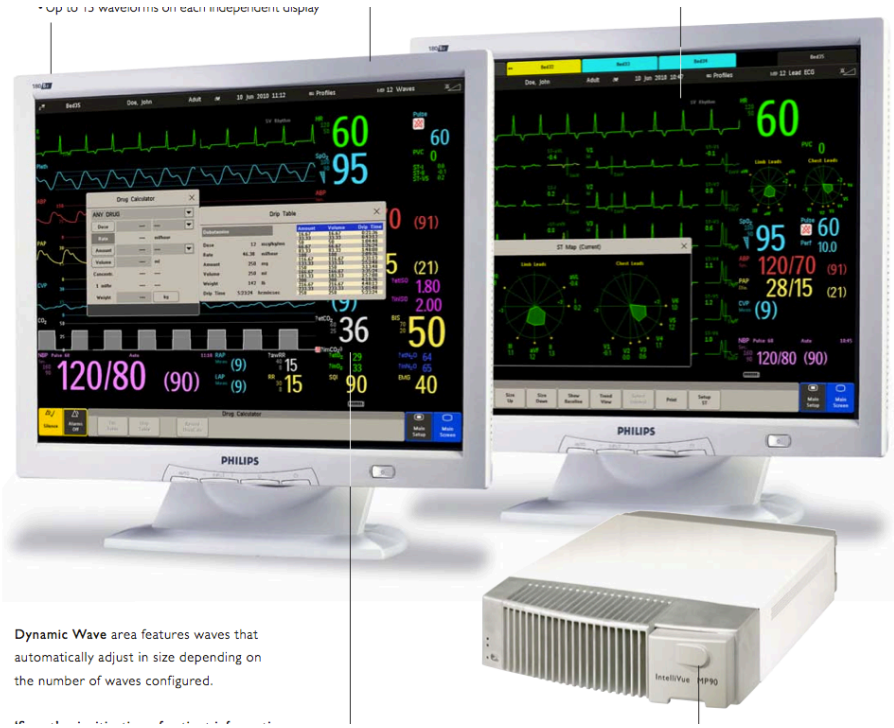
High-level presentation of issues related to architecture/regulation – not specific solutions

- Clinical motivation for cyber-physical systems of systems
  - See also talks from Dr. Julian Goldman
- Concept of a Medical Application Platform (MAP)
- Distinguishing characteristics of MAPs
- Integrated Clinical Environment – an architectural standard for MAPs
- Medical Device Coordination Framework (MDCF) – an open source framework for prototyping MAP concepts



Current Products

Current connectivity products *use proprietary interfacing* and many *limit components* to those from a single vendor or limited collection of vendors



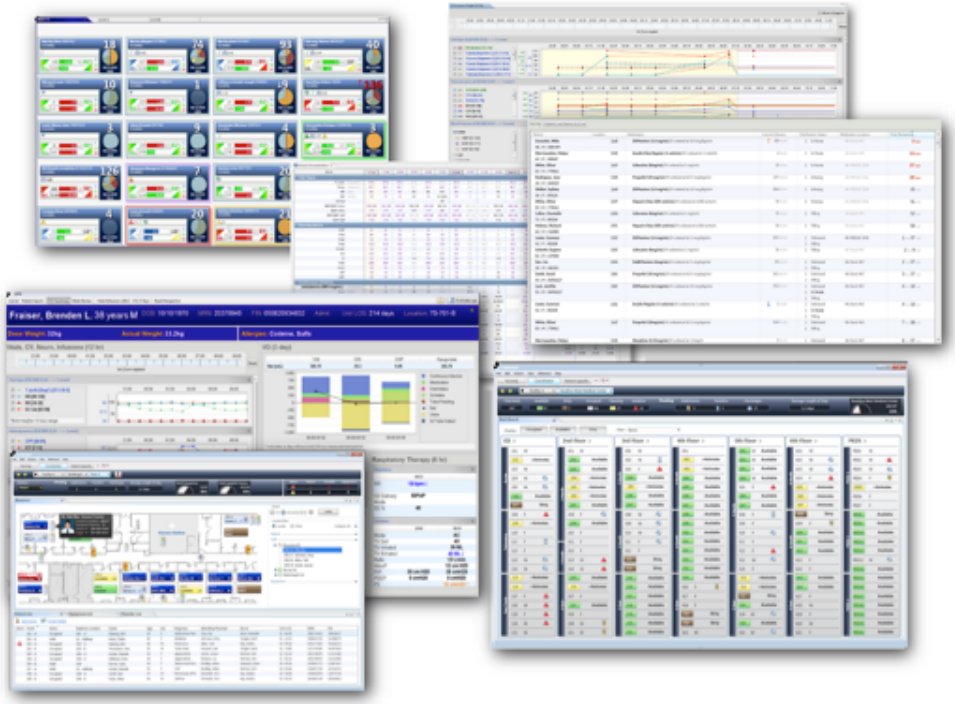
For example, Philips MP90 networked monitoring solution integrates *with other Philips* products in the IntelliVue line, or pulse oximeters from Masimo and Nellcor. *Note:* IntelliVue is not a MAP; it does not support app-based behavioral configuration.

Current Trends

Example Trend: Cerner MDDS iAware App Store

CareAware iAware® Application Platform

"Organizations are able to purchase gadgets and perspectives from the Cerner Store as well as write and publish their own gadgets. The iAware platform supports the ability to plug these gadgets and perspectives into views to create a customized application based on the needs of a specific organization, role or venue." – Cerner Marketing Material

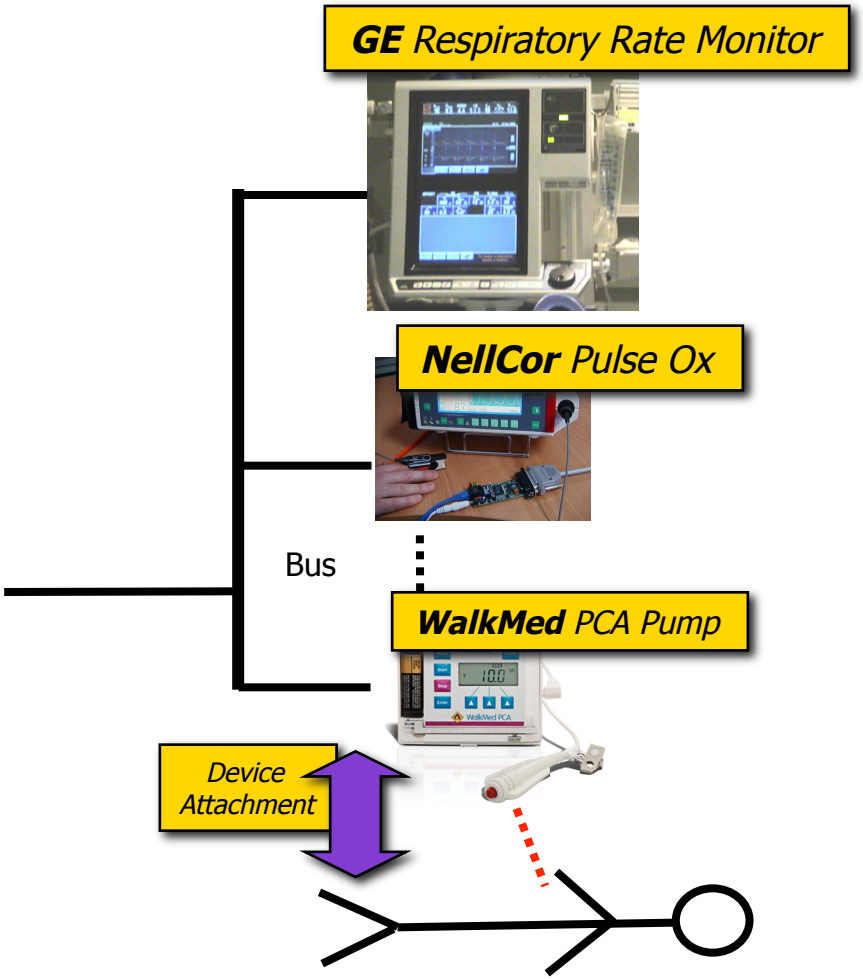


Note: iAware is essentially an MDDS (data forwarding) platform (though it does have a 510(k), not a full device coordination (ICE-like) platform. However, it provides a foundation for moving toward concepts embodied in a medical application platform.

MAP System Characteristics

MAPs should support *interoperability* with *heterogeneous components*

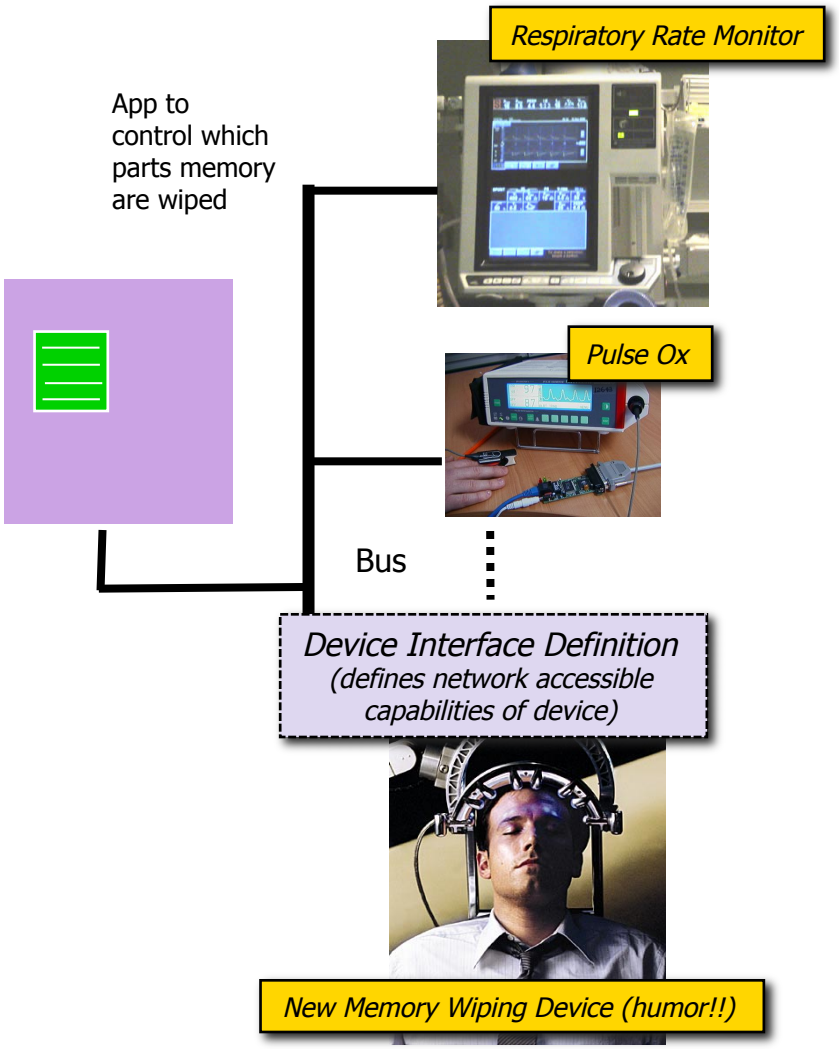
- MAP should support components produced by different vendors
  - Different quality management systems
  - Tension between accessible risk management file and proprietary information
- Success of the MAP approach depends on individual vendors being willing to…
  - Pursue interoperability as a business strategy
  - Conform to (envisioned) open interfacing & safety standards
- **Note**: These goals may be scaled back to a smaller eco-sphere, e.g., managed by a single vendor



MAP System Characteristics

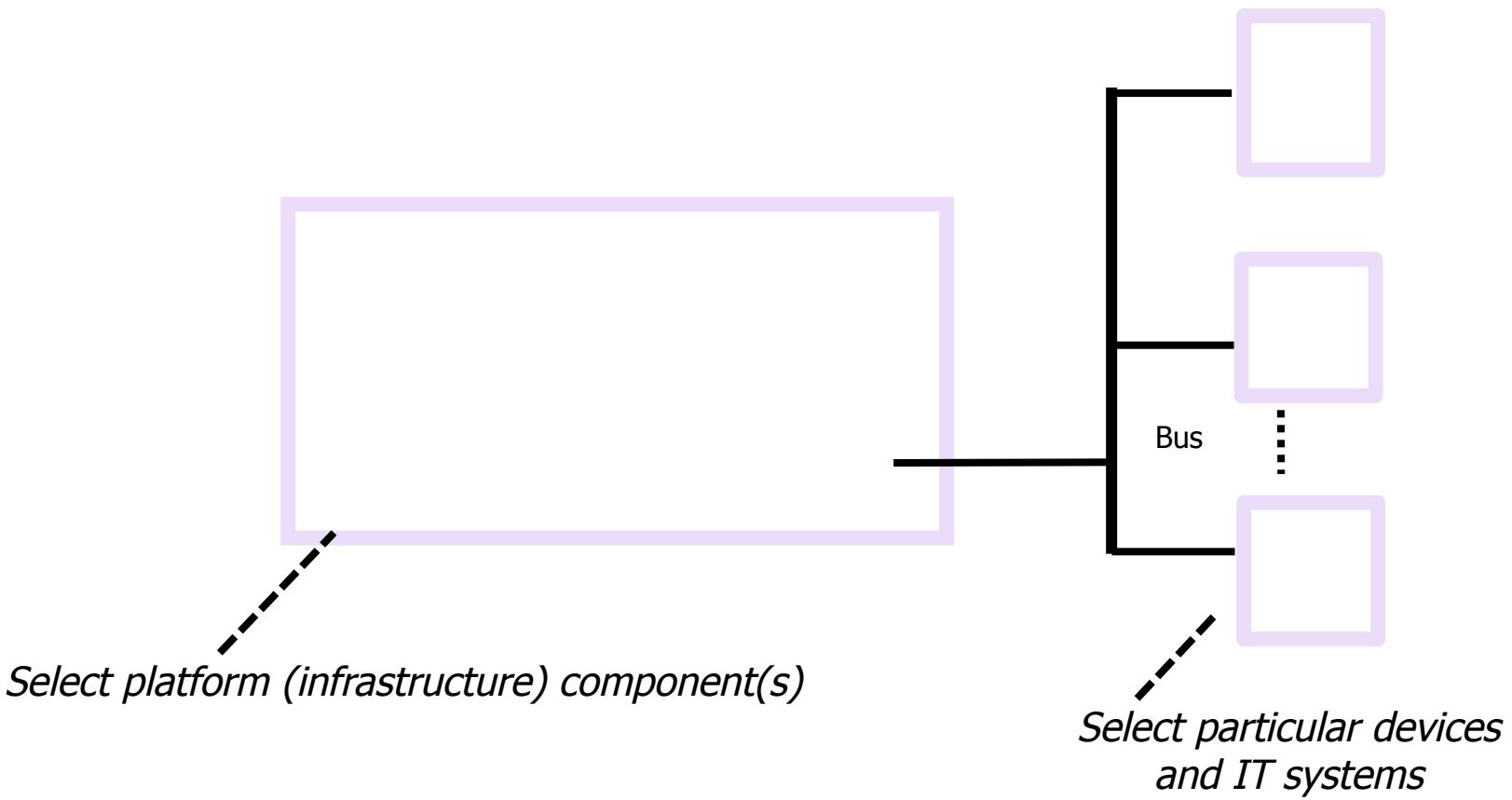
MAPs are *open and extensible* – new devices and apps that were unknown when the platform was developed/approved can be incorporated

- When most conventional critical systems are deployed, the set of possible constituents is known in advance.
- MAP infrastructure is developed and deployed…
  - …subsequently used to support new devices, new device types, and apps that were not anticipated at the time of development, V & V, and regulatory approval
- Relies on the fact that the MAP provides…
  - …an interface definition language (IDL) that devices uses to describe their capabilities
  - …an app language that developers use to write apps
- Because the MAP is verified to support the IDL and app language, it can work with any device/app whose capabilities/function can be described in those languages.



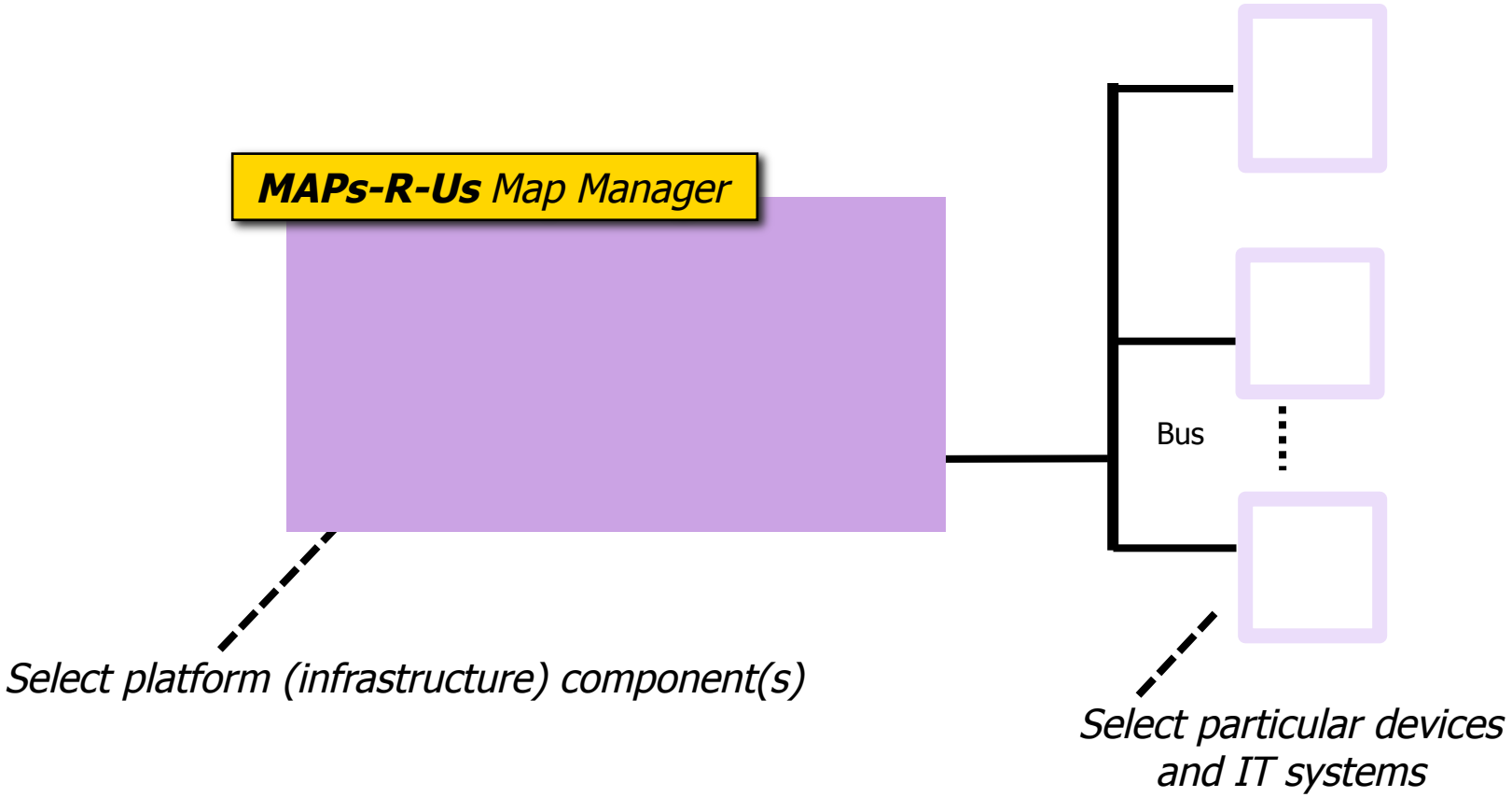
MAP Instance

A *MAP instance* is an instantiation of the MAP architecture – i.e., a selection of specific MAP hardware components that conform to specific architectural and interfaces specified (standardized!) by the MAP framework.



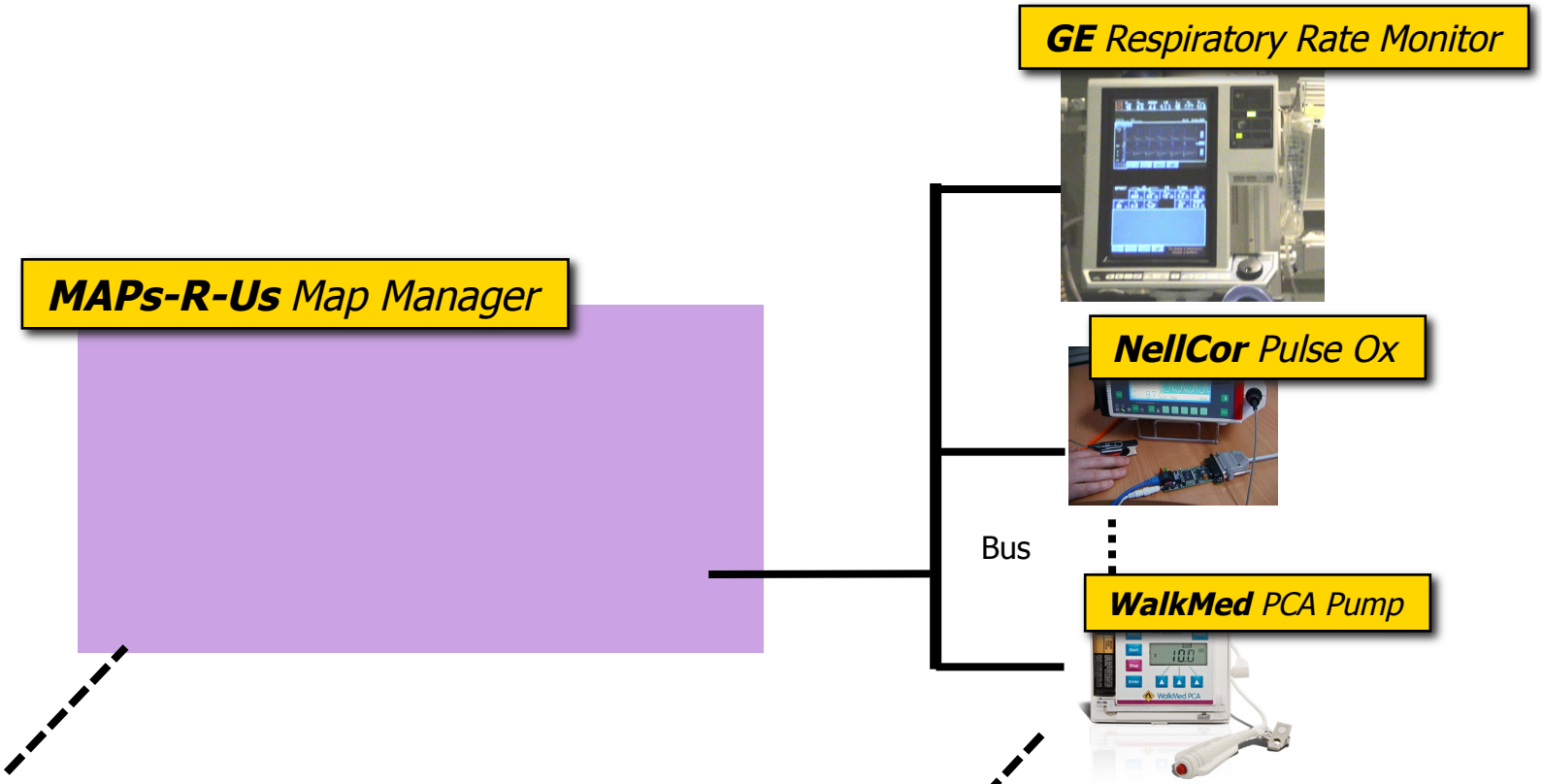
MAP Instance

A *MAP instance* is an instantiation of the MAP architecture – i.e., a selection of specific MAP hardware components that conform to specific architectural and interfaces specified (standardized!) by the MAP framework.



MAP Instance

A *MAP instance (deployment)* is an instantiation of the MAP architecture – i.e., a selection of specific MAP hardware components that conform to specific architectural and interfaces specified (standardized!) by the MAP framework.



Select platform (infrastructure) component(s)

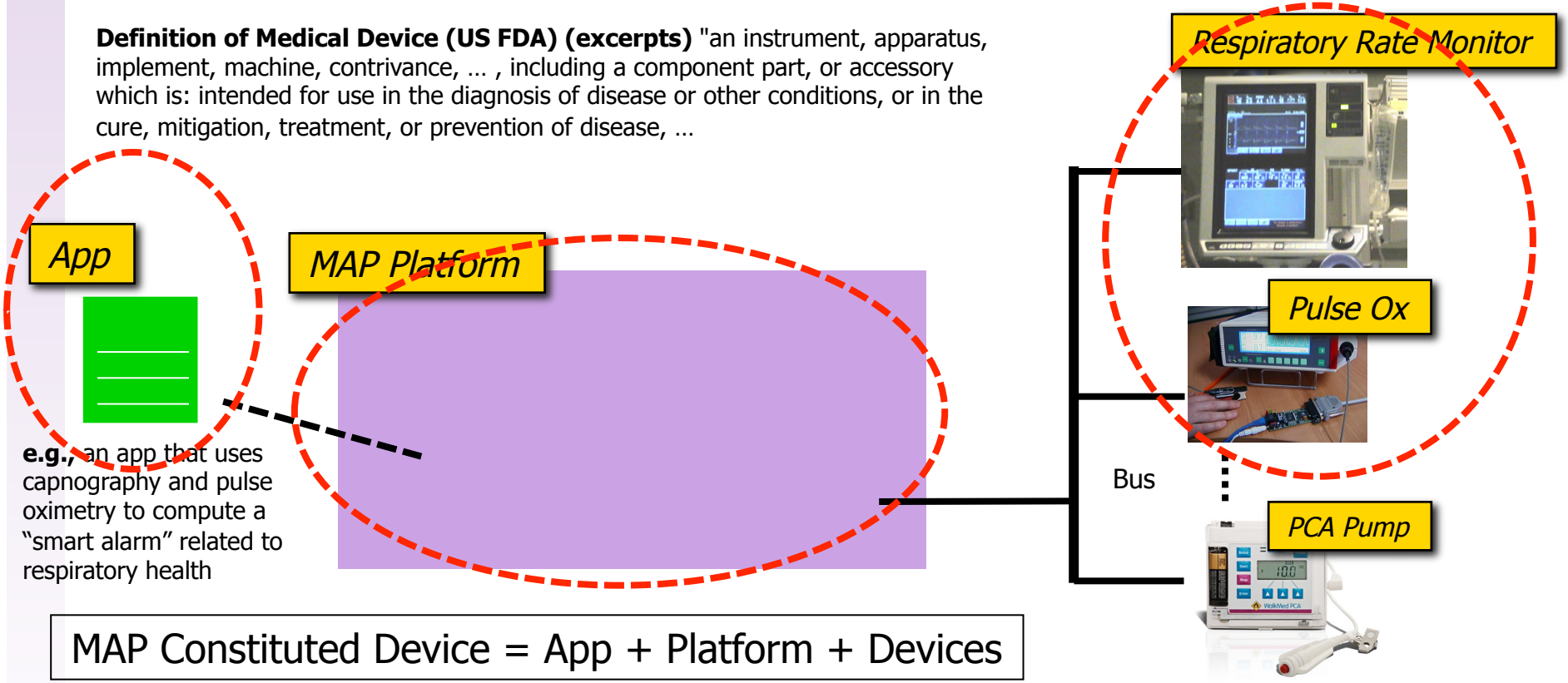
Select particular devices and IT systems

What are we regulating / verifying? The architecture? An instance? All possible instances? What exactly constitutes the *medical device* whose safety and effectiveness we are interested in?

MAP Constituted Device

A *MAP constituted device* is the (composite, virtual) device/system behavior obtained by running an app on a particular MAP instance. The device is conceptual until the app is launched.

Definition of Medical Device (US FDA) (excerpts) "an instrument, apparatus, implement, machine, contrivance, … , including a component part, or accessory which is: intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, …



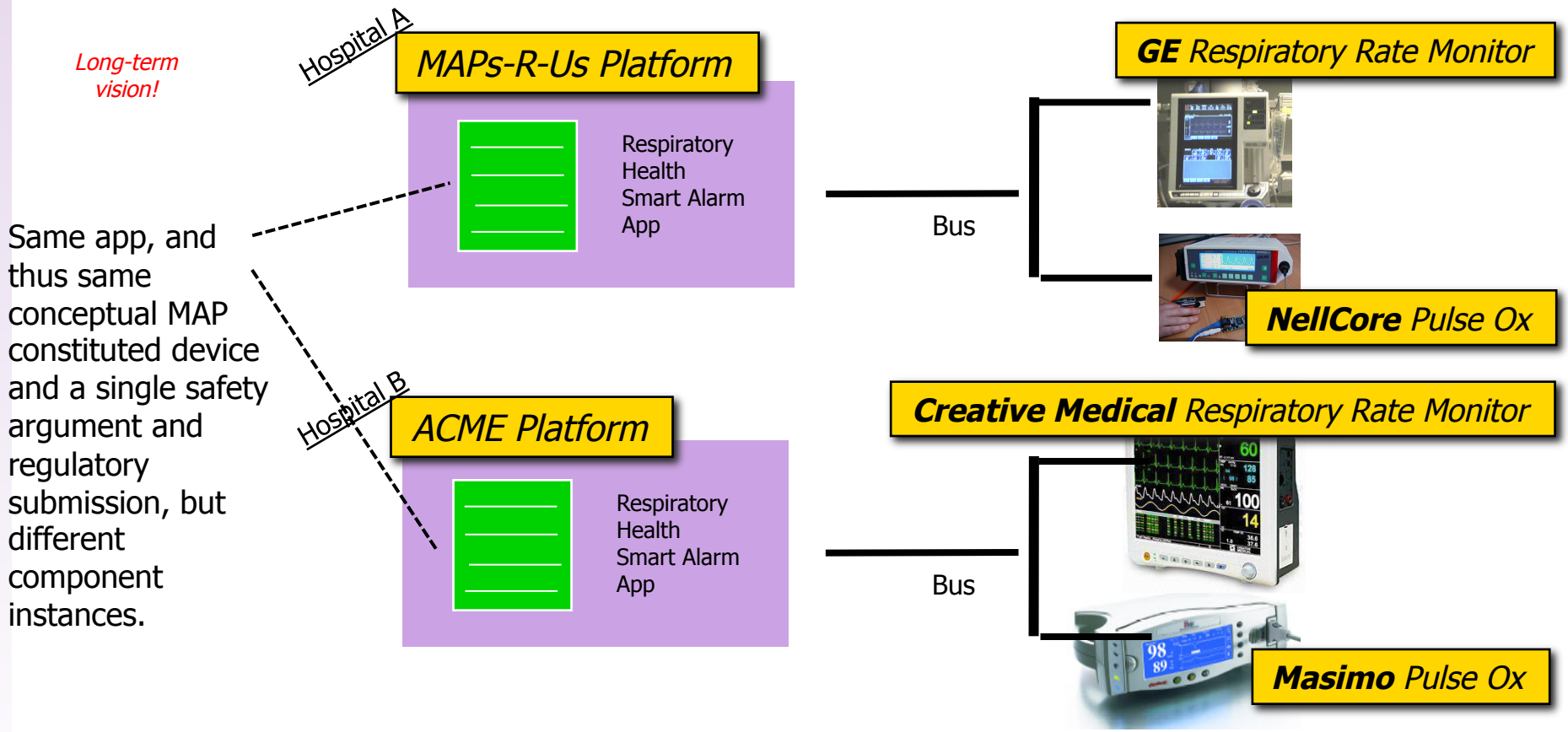
e.g., an app that uses capnography and pulse oximetry to compute a "smart alarm" related to respiratory health

MAP Constituted Device = App + Platform + Devices

No one of these entities defines the behavior of the system alone – they each contribute behavior to the composite system. The app plays a special role – it *specifies* the composite behavior and thus defines the *clinical intended use* (regulatory term) of the MAP constituted device that results from running the app.

MAP Characteristics

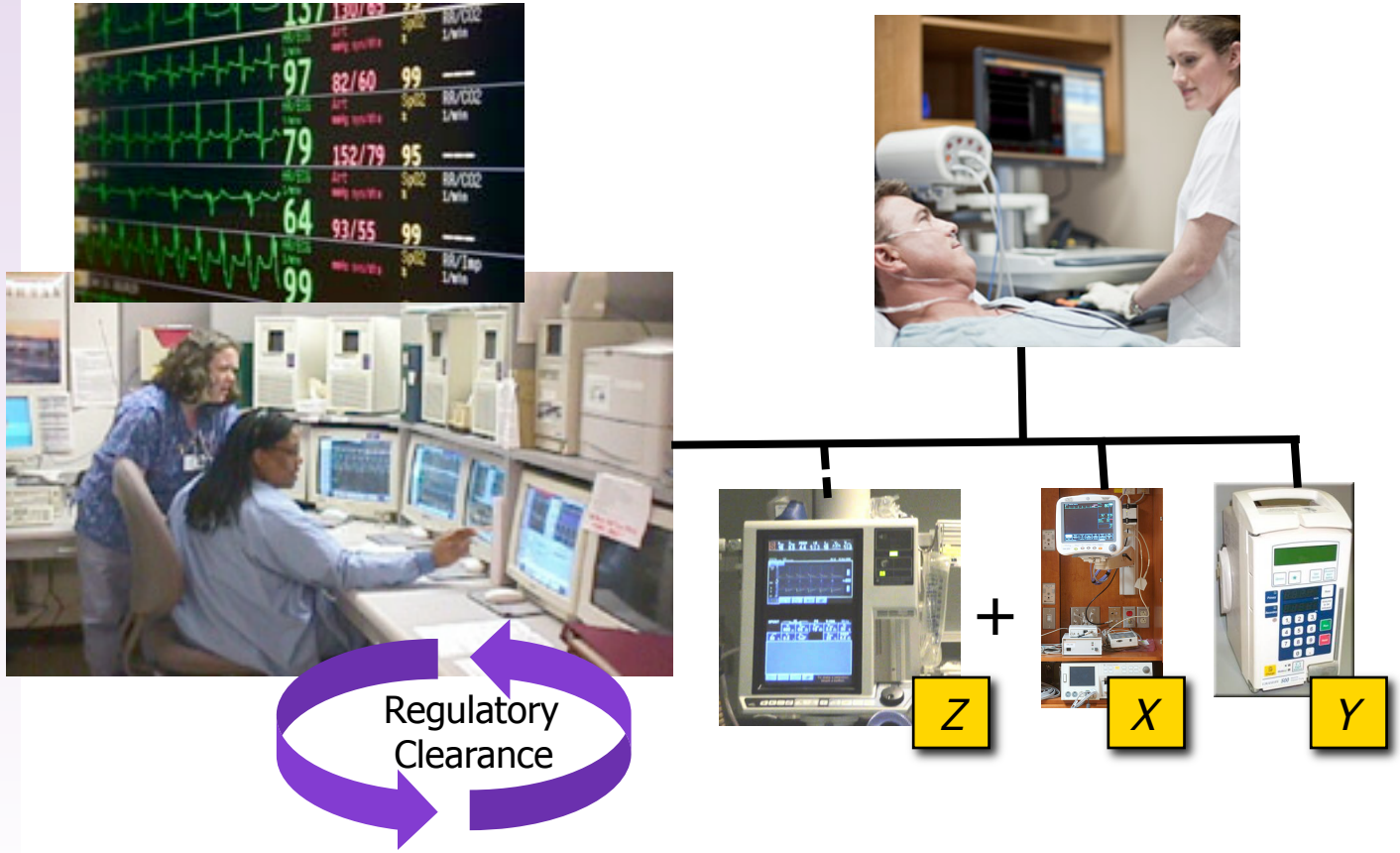
MAP constituted device instances are variable – the constituents that form the MAP constituted device may differ on different invocations of the device.



Implications: Possible variances/ranges in the behavior must be taken into account by the device interfacing strategy, by the app and its associated safety arguments. Some devices may not meet the apps requirements and should be rejected by platform services.

Needed: New Regulatory Approach

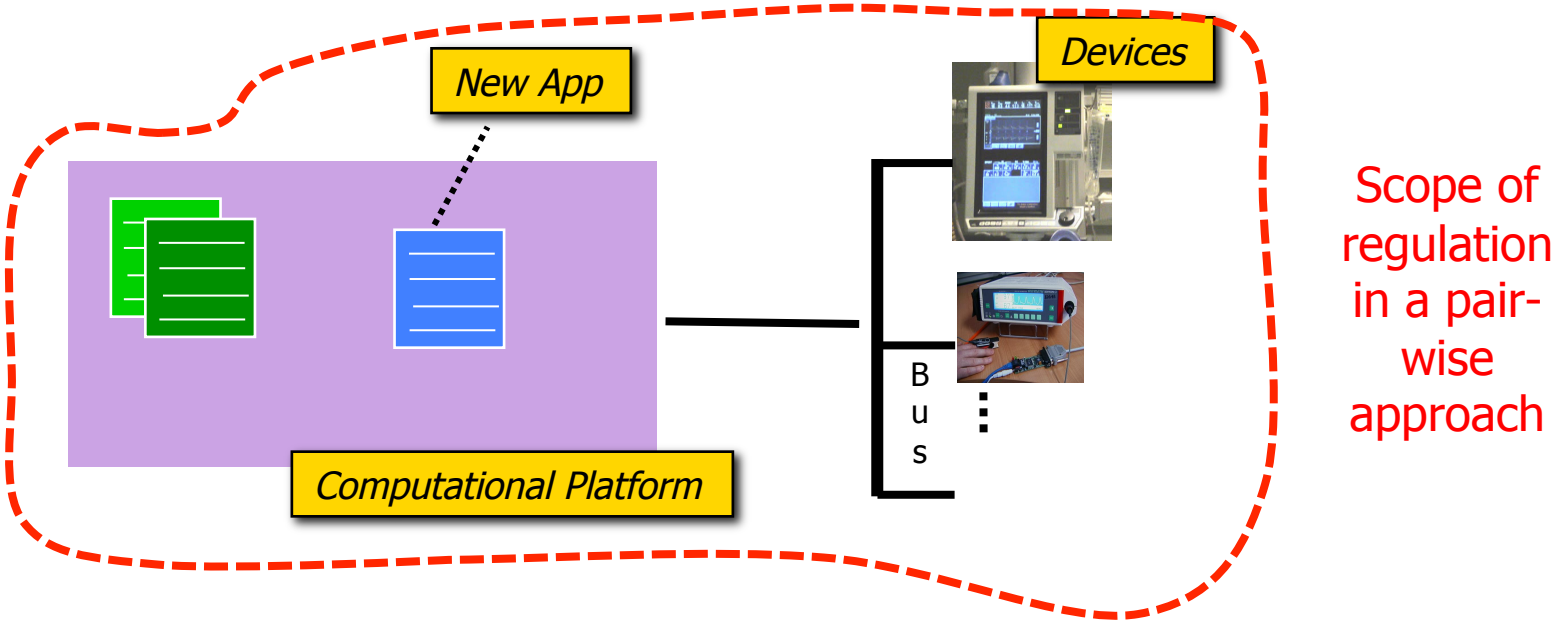
Current regulation of integrated systems (e.g., central station monitors) typically requires **"pair-wise" clearance**: whenever a new type of device is added to the monitoring platform, the entire infrastructure must be re-cleared.



Assume monitoring system was originally developed, verified, and received regulatory clearance for devices of type X & Y.

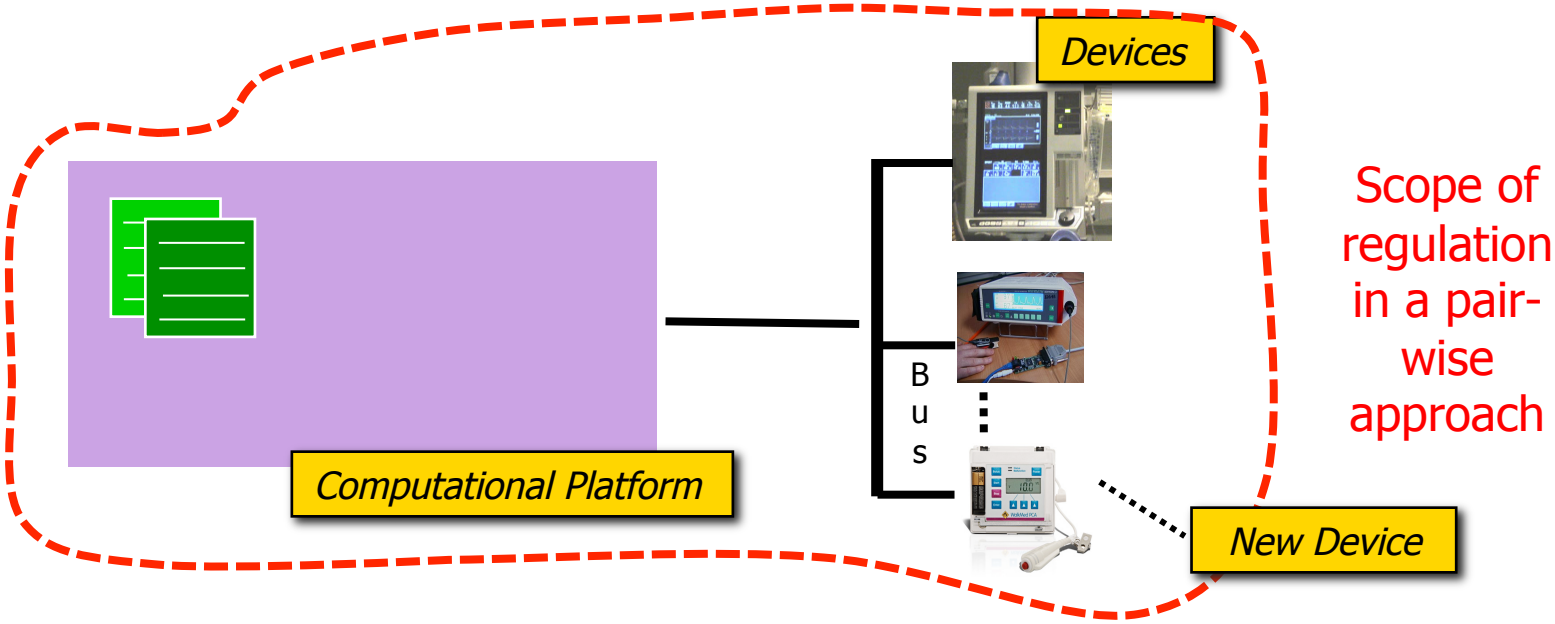
In current regulatory approach, adding a new type of device (e.g., Z) typically causes the entire system to be re-submitted for regulatory clearance.

Needed: New Regulatory Approach



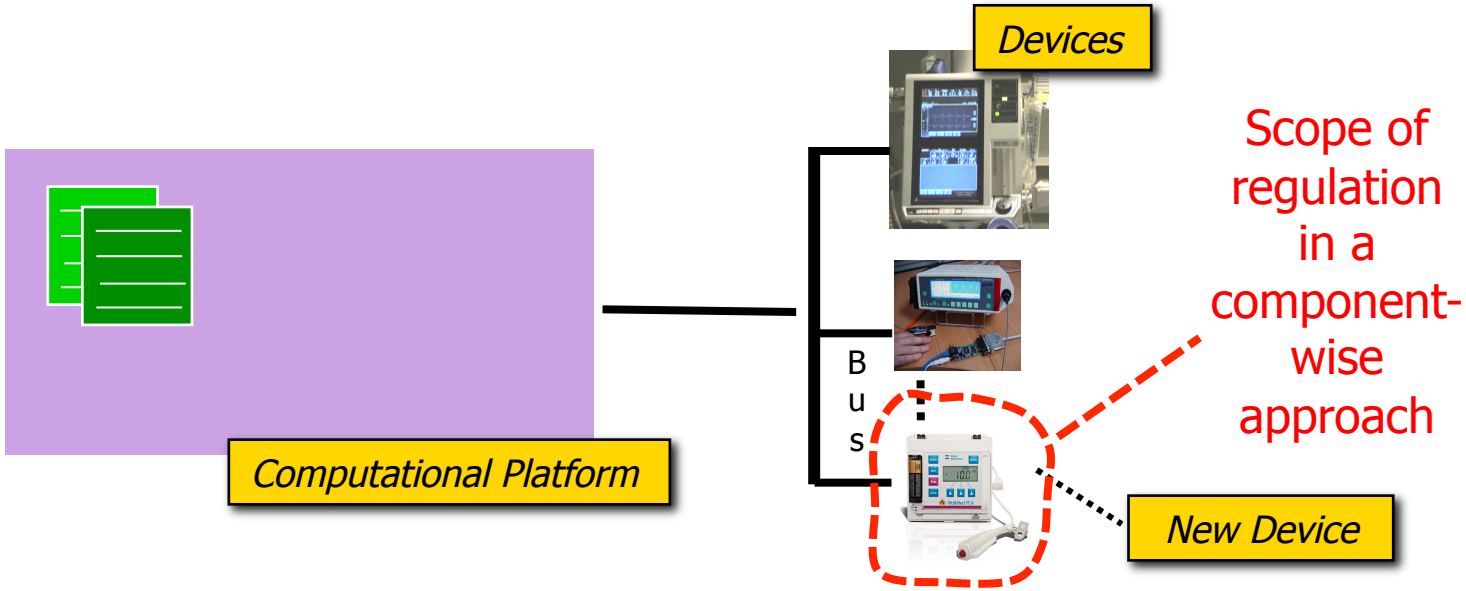
- In the current "pair-wise" regulatory approach, when adding a new app…
  - …the scope of regulation would be the entire system
  - …i.e., set of all MAP instances and app would need to be submitted for regulatory approval

Needed: New Regulatory Approach



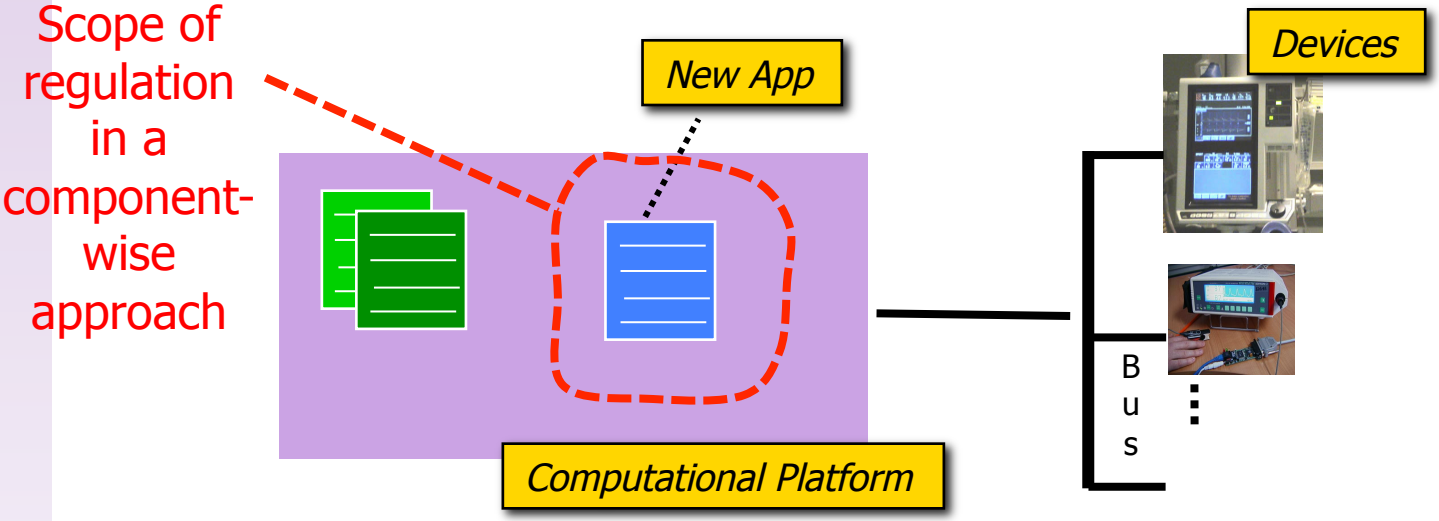
- In the current "pair-wise" regulatory approach, when adding a new device…
  - …the scope of regulation would be the entire system
  - …i.e., set of all MAP instances and device would need to be submitted for regulatory approval

Envisioned Compositional Approach



- In an envisioned "component-wise" regulatory approach, when adding a new device…
  - …the scope of regulation would be the device and its MAP interface
    - Does it appropriately declare its capabilities?
    - Does it appropriately declare hazards, safety-states?
    - Does it appropriately implement the MAP networking protocols?

Envisioned Compositional Approach



- In an envisioned "component-wise" regulatory approach, when adding a new app…
  - …the scope of regulation would be the just the app
  - …the app specifies its requirements for devices and platform capabilities (which would be checked by the platform at launch time)
  - …the app regulatory submission provides an overall argument for safety of the constituted device

Component-Wise: Limits?

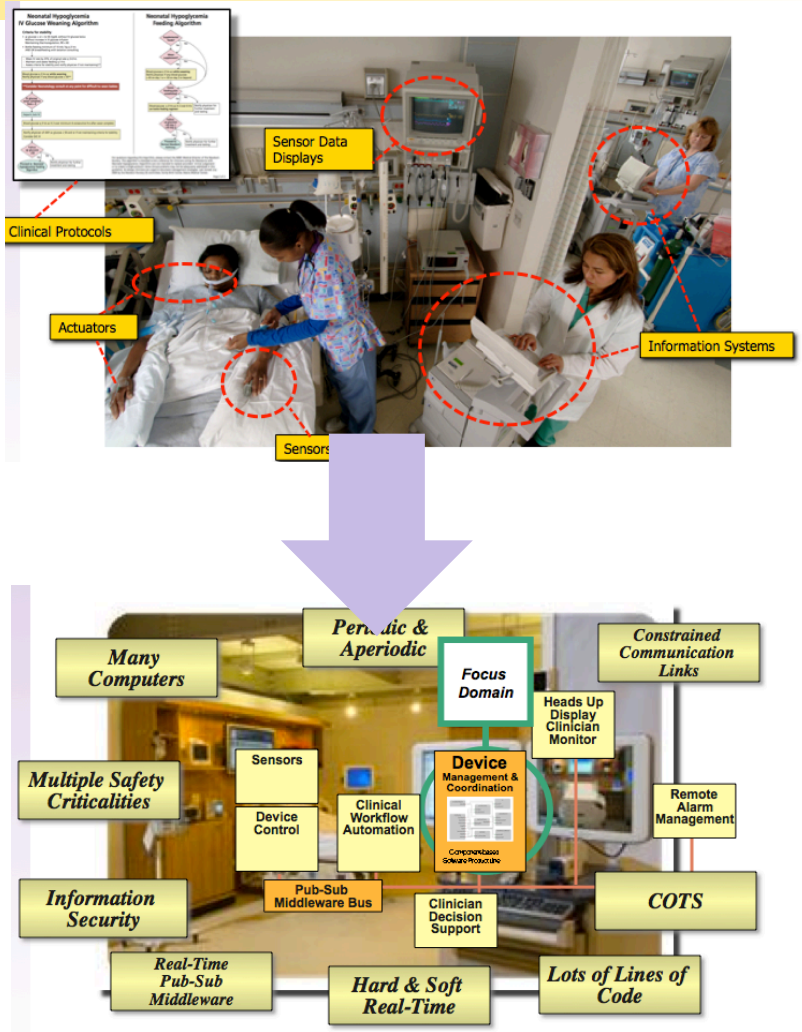
Currently the safety and engineering principles for determine when component-wise review can be applied (and when it should not be applied) are unclear

- FDA currently permits some notions of component-wise review
  - Decisions made on an ad hoc basis
  - No explicit statement of safety principles that justify when such an approach can be taken
  - Creates uncertainty in vendor space
    - "Could I apply this to my product?"
    - "What steps do I have to take to allow my product to be reviewed in this way?"
  - Creates uncertainty for the regulator
    - "What exactly do I look for in this submission?"
    - "On what technical basis should I grant approval or deny approval?"
- Our research and activities in standards work are aiming to systematically enumerate the architecture, interface, risk management, V&V principles necessary to support component-wise review in interoperable systems
  - …clarify when component-wise review should be allowed and when it should not be allowed

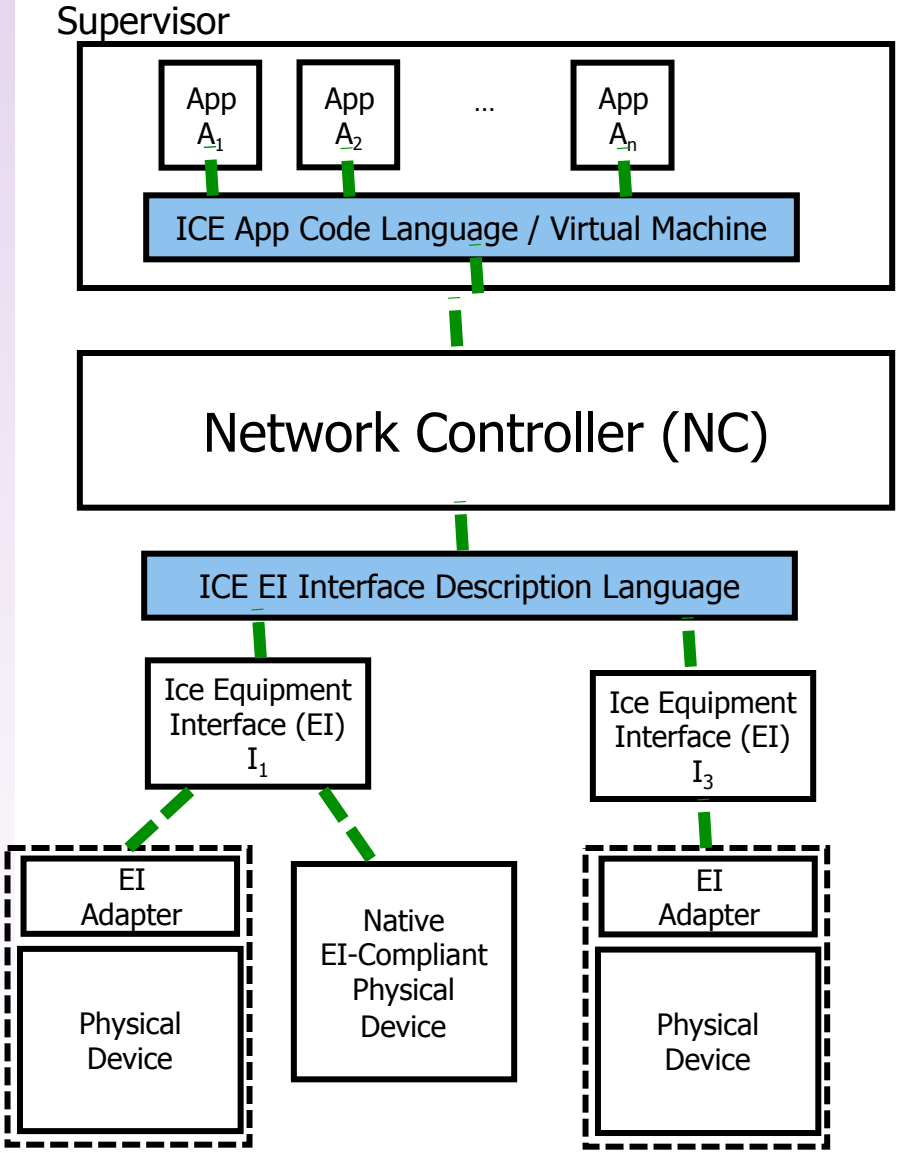
This Talk

High-level presentation of issues related to architecture/regulation – not specific solutions

- Clinical motivation for cyber-physical systems of systems
  - See also talks from Dr. Julian Goldman
- Concept of a Medical Application Platform (MAP)
- Distinguishing characteristics of MAPs
- Integrated Clinical Environment – an architectural standard for MAPs
- Interoperability Safety Standards (AAMI / UL 2800)

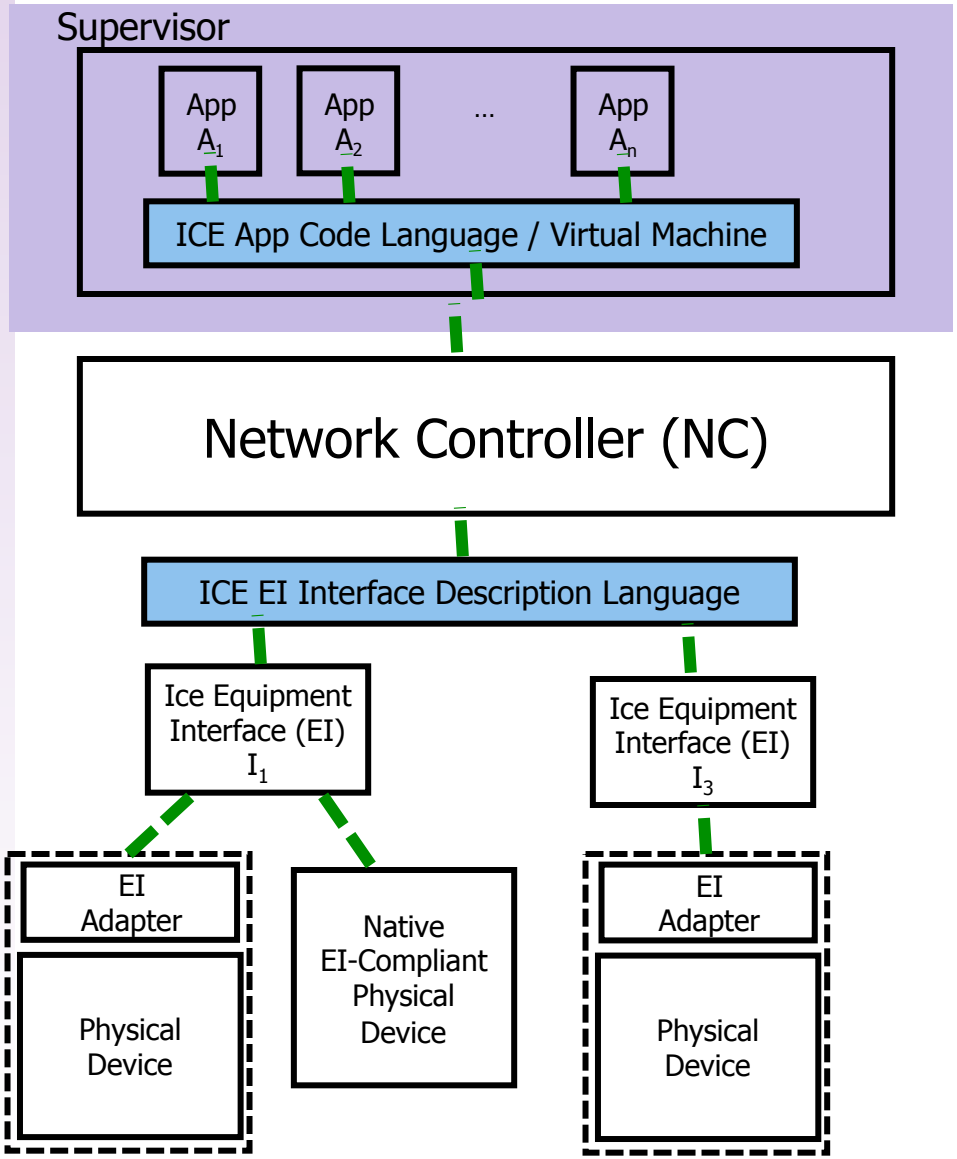


Integrated Clinical Environment



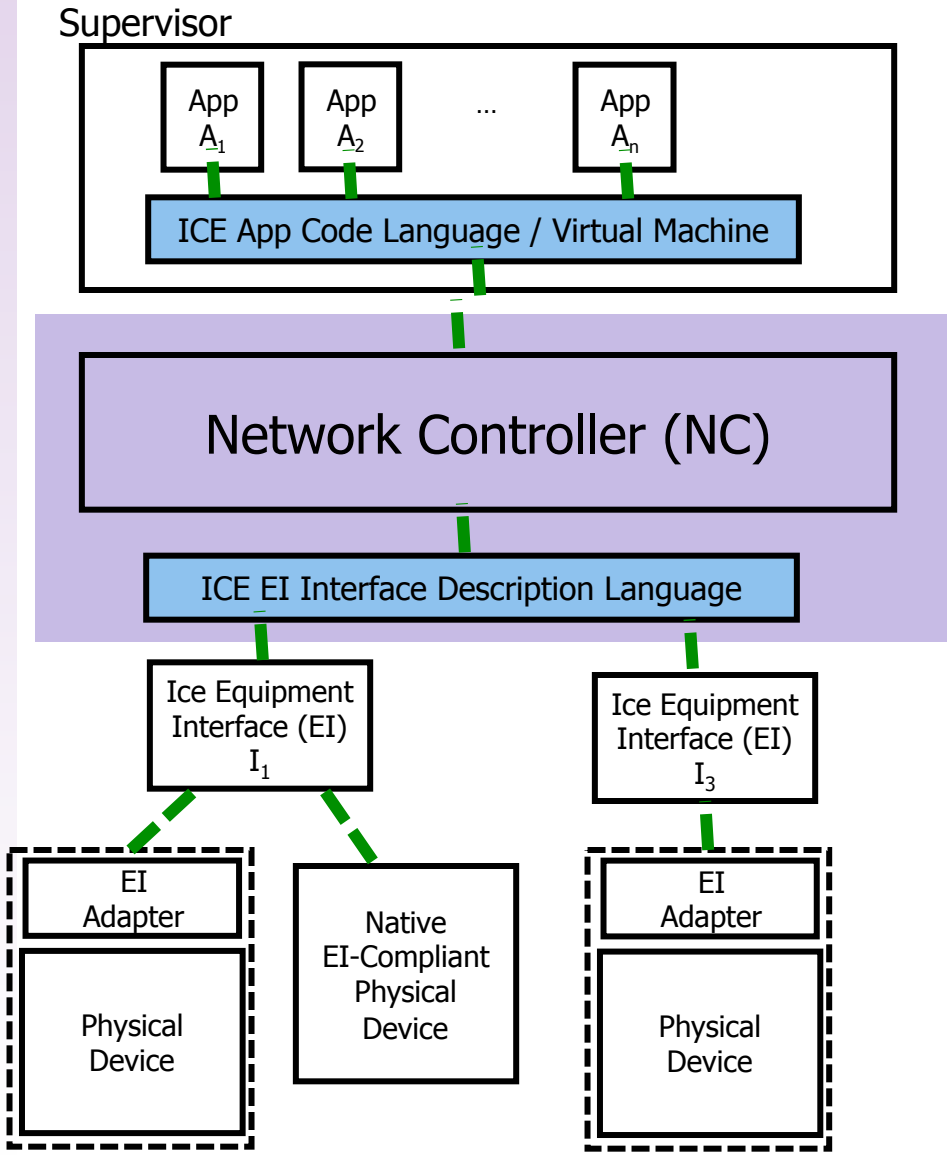
- ASTM Standard F2761-2009 for ICE defines a high-level architecture and functional concept
- Subsequent standards are intended to provide specific functional and interfacing requirements for components
- ASTM F2761 is one of a collection of standards related to interoperability recognized by the FDA, and the only one of the collection that address architectural concerns
- ICE architecture standard is the focal point of multiple standards development effort in the medical device community (AAMI, UL)

Supervisor Concept/Goals



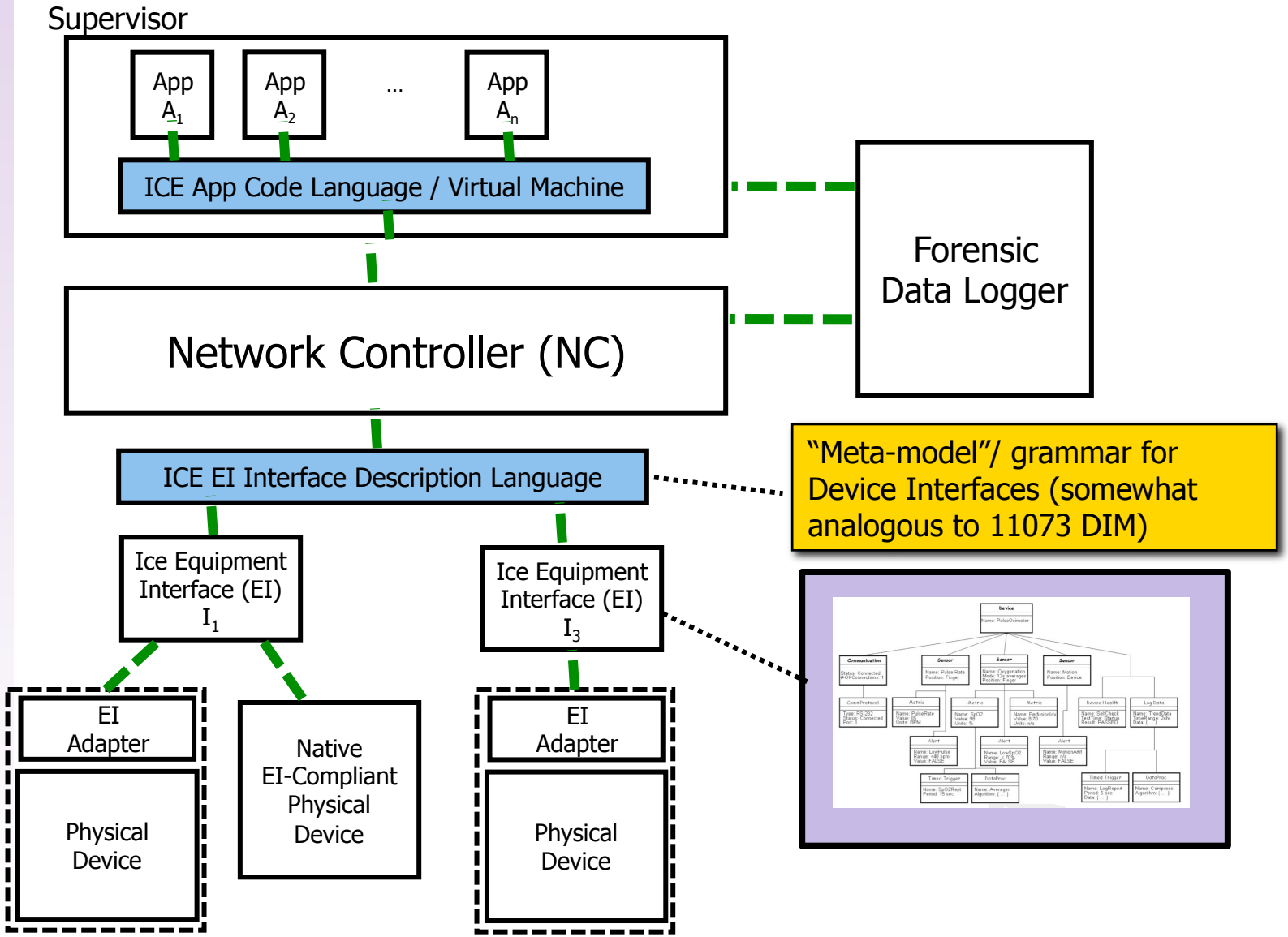
- Provides virtual machine functionality to host apps
- Application Program Interfaces (APIs) for…
  - clinical displays
  - determining what devices are available on the network for apps to use
  - exchanging data between apps/devices
  - exchanging data between apps and EMR and other health IT systems
- Services that allow apps to be notified when important system faults occur such as…
  - unanticipated device disconnected
  - failed or slow delivery of messages between devices / apps
- Run-time checking to ensure that apps …
  - are "well-behaved"
  - don't interfere with each other in unanticipated ways

Network Controller Concept/Goals



- High assurance network & services to support communication between apps, devices, and health IT systems
- Often built using "publish/subscribe" middle that provides virtual "information channels" with configurable security and performance
- Exposes the ICE interfaces of attached devices to apps
  - Handles app requests to read/write to device interfaces with appropriate access/concurrency control
  - Keeps track of devices on network and device connections and notifies associated apps when problems occur
- Manages the discovery and connection protocol of devices that desire to connect to the ICE
  - *Authentication* ensures that only devices that have been previously certified as ICE compliant can connect/associate

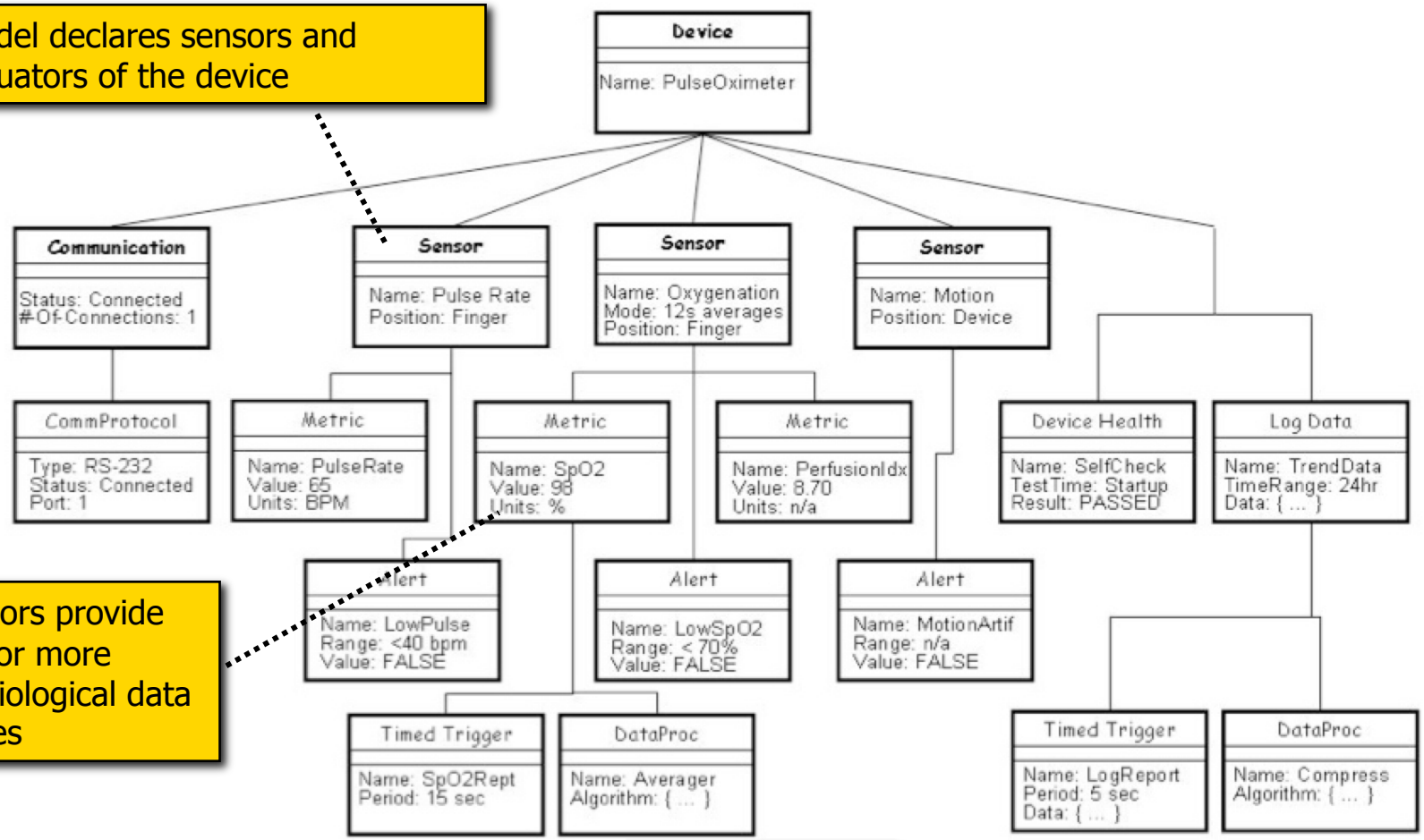
Device Interfacing Technology



ICE Device Model Concepts

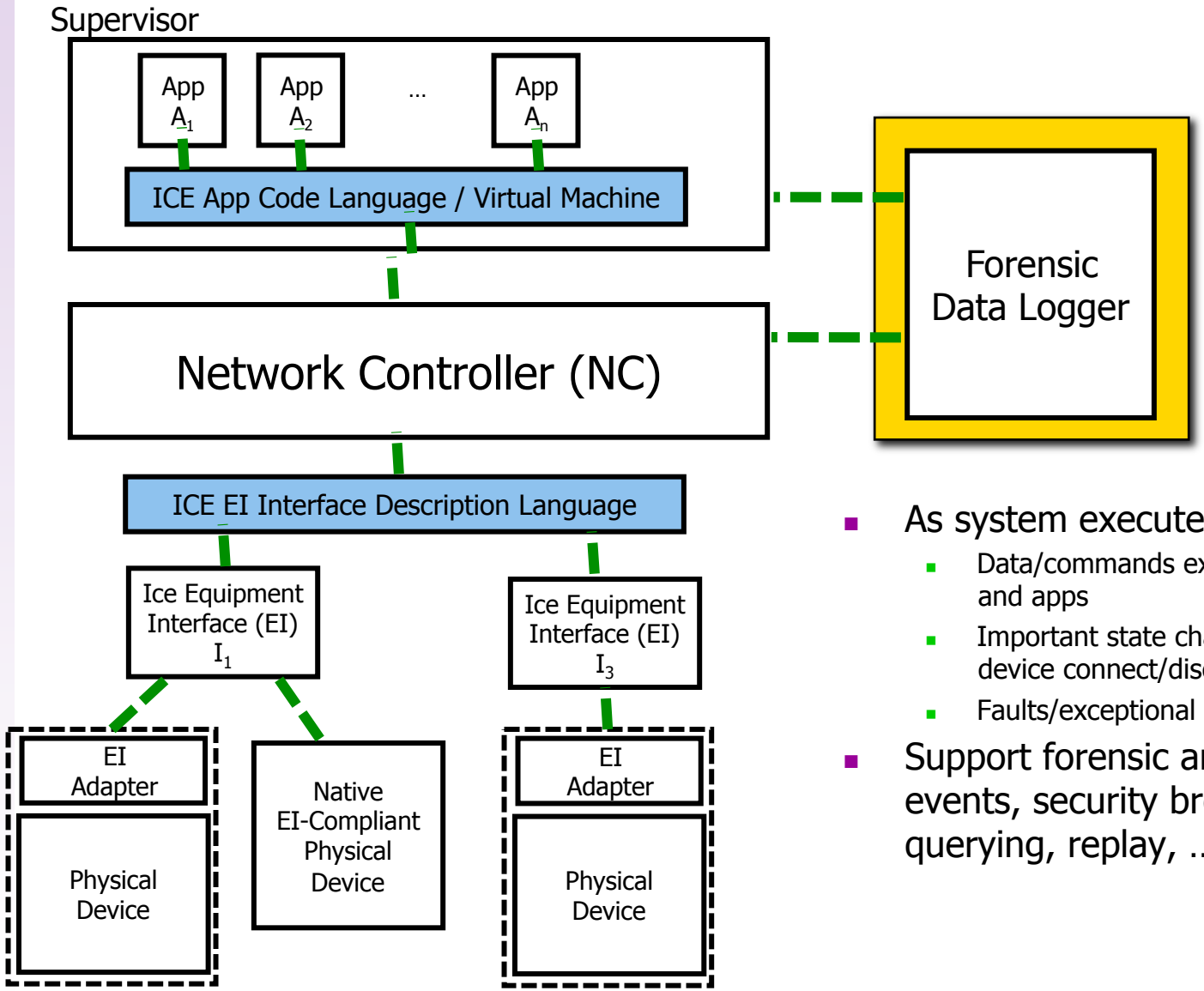
Device Model will provide a declarative (ontology-oriented) description of a devices capabilities that will be exposed to apps

Model declares sensors and actuators of the device



Sensors provide one or more physiological data values

Data Logger Concept/Goals

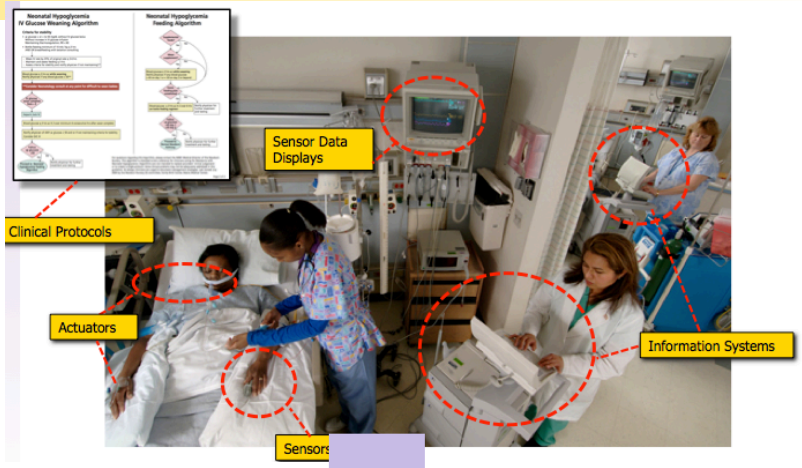


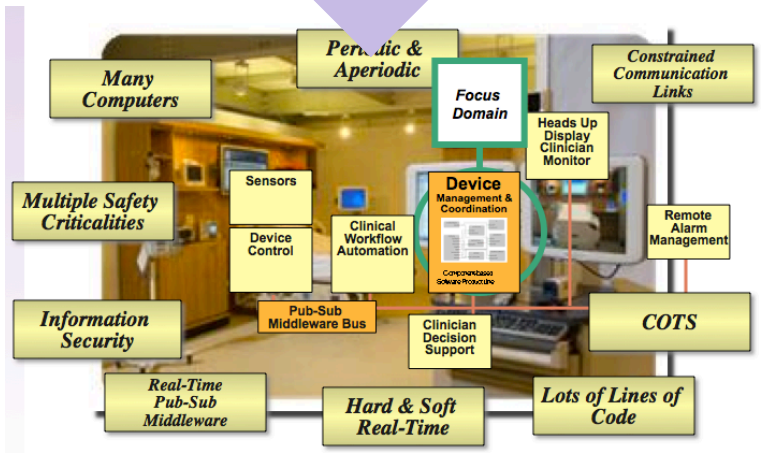
- As system executes, log…
  - Data/commands exchanged between devices and apps
  - Important state changes in the system (e.g., device connect/disconnect, app launch)
  - Faults/exceptional conditions
- Support forensic analysis of adverse events, security breaches, etc. via querying, replay, …

This Talk

High-level presentation of issues related to architecture/regulation – not specific solutions

- Clinical motivation for cyber-physical systems of systems
  - See also talks from Dr. Julian Goldman
- Concept of a Medical Application Platform (MAP)
- Distinguishing characteristics of MAPs
- Integrated Clinical Environment – an architectural standard for MAPs
- Interoperability Safety Standards (AAMI / UL 2800)

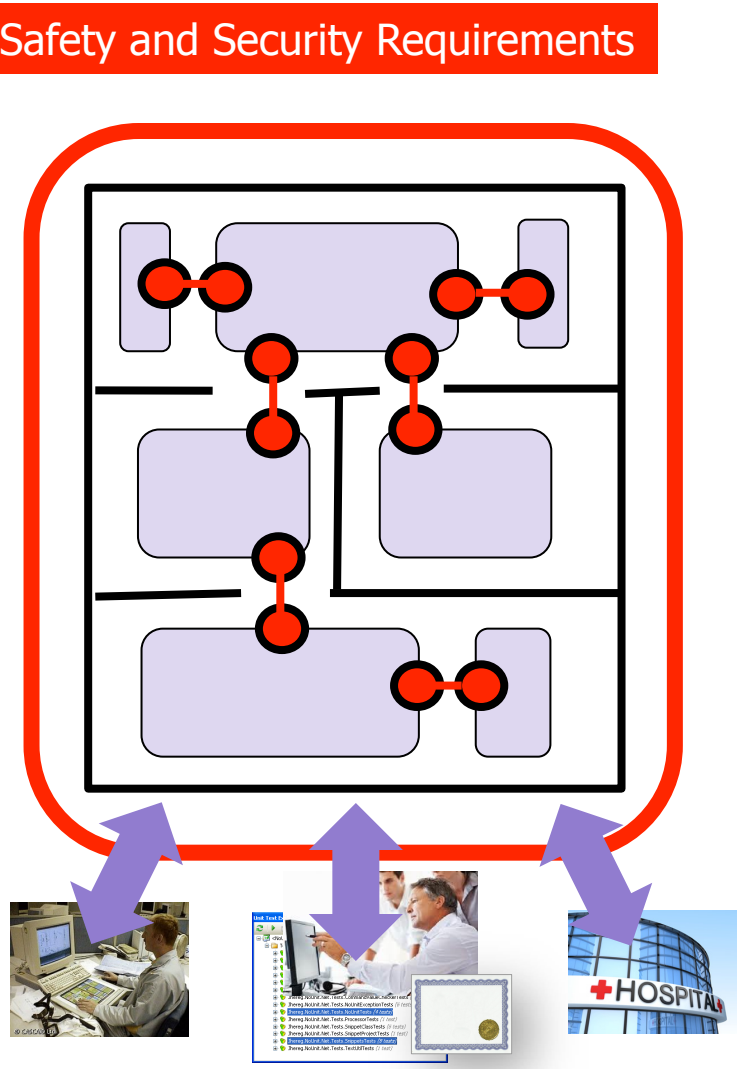




Goals of AAMI / UL 2800

Safety / Security Requirements for Multi-vendor Plug-and-Play Interoperability

- Component safety claims *in the context of system safety claims*
- Components assembled within
  - an architectural framework that constrains interactions
  - an organized ecosphere of stakeholders and processes that govern
    - interactions between stakeholders
    - contributions to systems



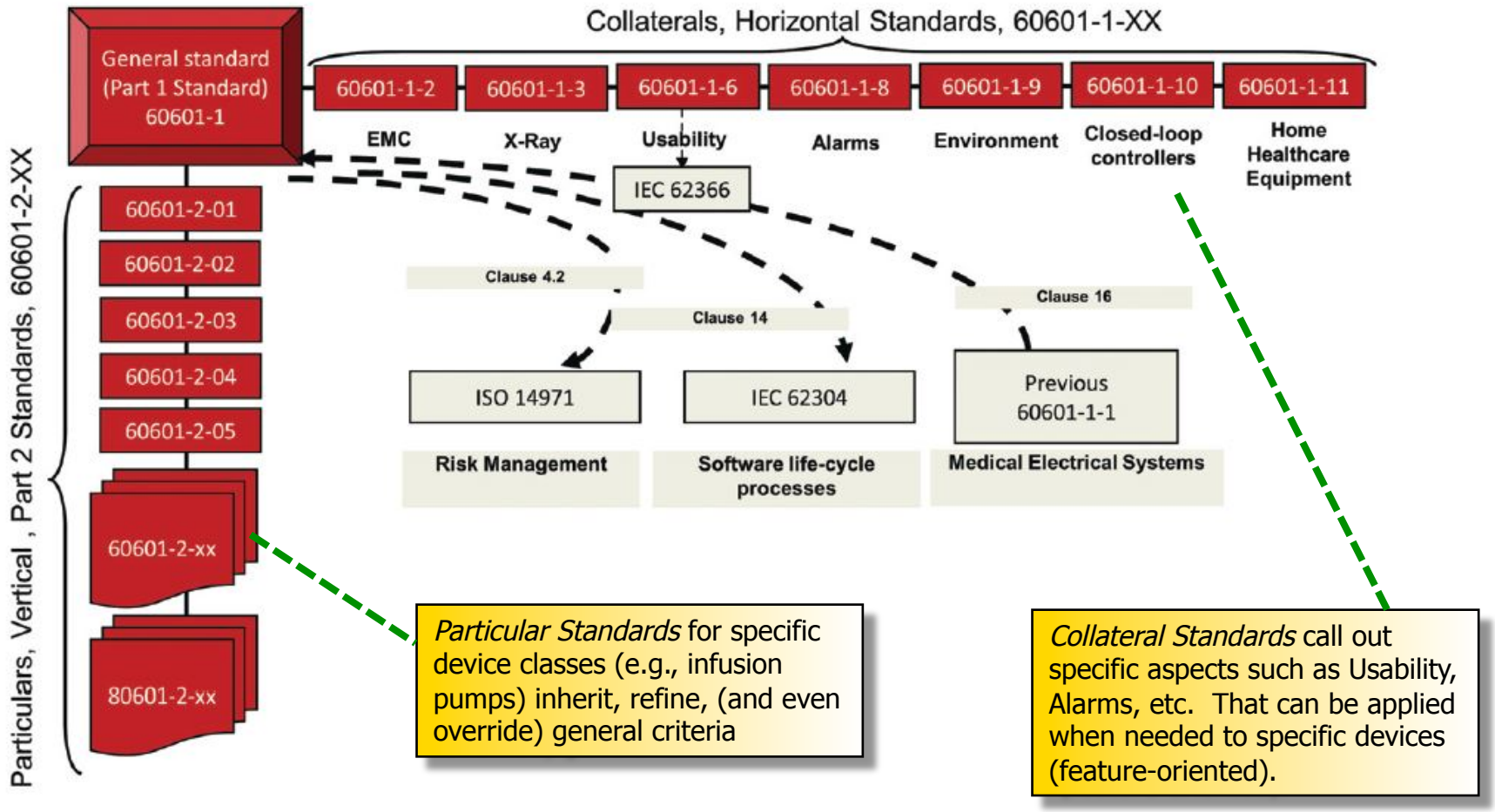
Goals of AAMI / UL 2800

Broad contributions of the 2800 family of standards

- provides requirements that can be applied within a medical system's safety lifecycle
- provides an approach for risk reduction consistent with risk management processes used in the medical device domain;
- provides a common set of system Safety, Security, and Essential Performance objectives for which to target risk reduction activities;
- provides guidance for developing and documenting system architectures and interfaces so that safety and security of interoperable systems can be more easily achieved and demonstrated by constraining interactions and reducing unnecessary variability;
- provides safety-driven security requirements
- provides a technical basis for a component-wise approach to carrying out certain risk management activities and for establishing important classes of safety- and security-related properties in the content of appropriately defined architectures
- provides requirements for verification, validation, and confirmation measures based on evidence and explicit arguments, introducing language that points to the use of arguments/evidence in assurance cases to ensure a sufficient and acceptable level of safety and security is achieved.

Example of Standard Refinement

The 60601 family of medical device safety standards provides an example of standard refinement/aspect that allow more general requirements to be tailored to particular contexts…



Particular Standards for specific device classes (e.g., infusion pumps) inherit, refine, (and even override) general criteria

Collateral Standards call out specific aspects such as Usability, Alarms, etc. That can be applied when needed to specific devices (feature-oriented).

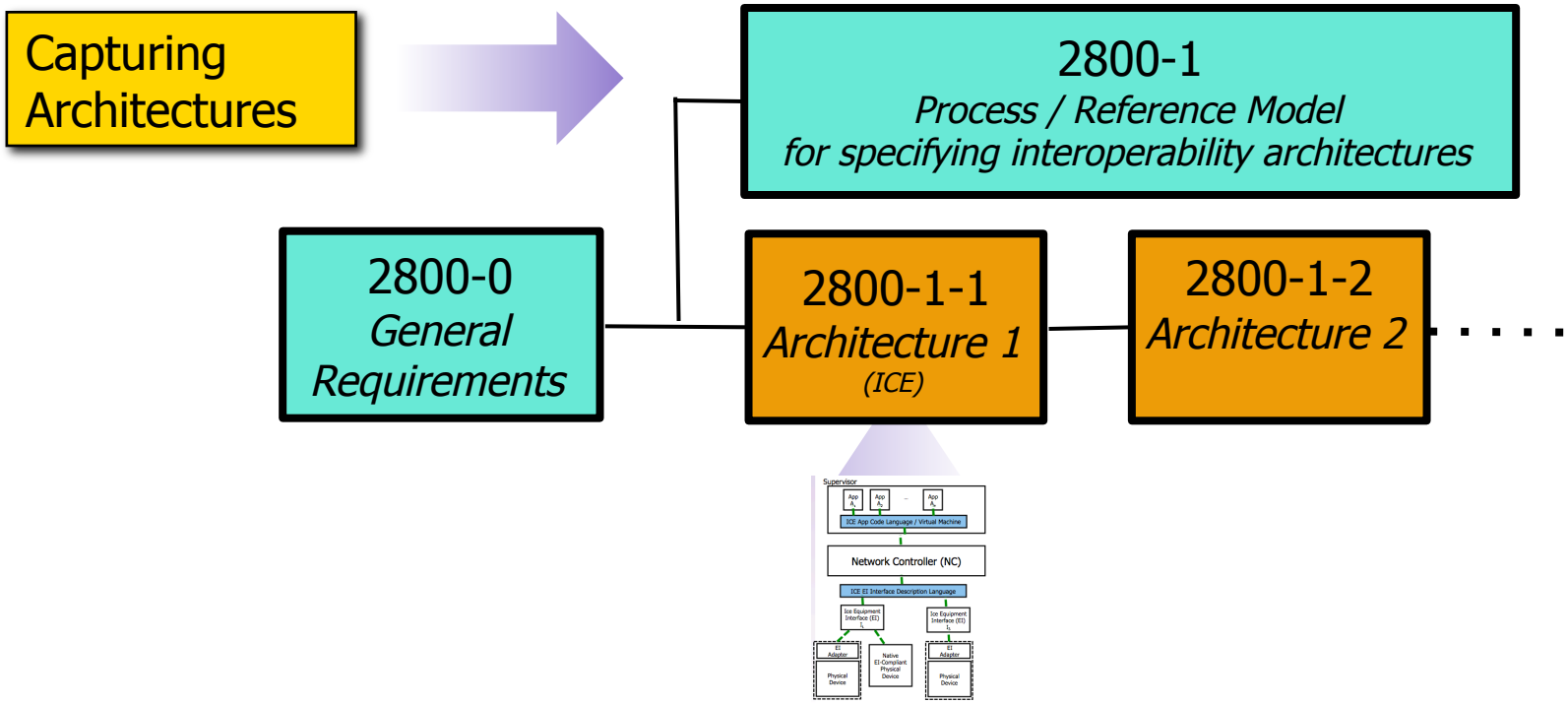
Proposed 2800 Structure

Capturing Architecture and Application Independent Safety/ Security Requirements

2800-0
General Requirements

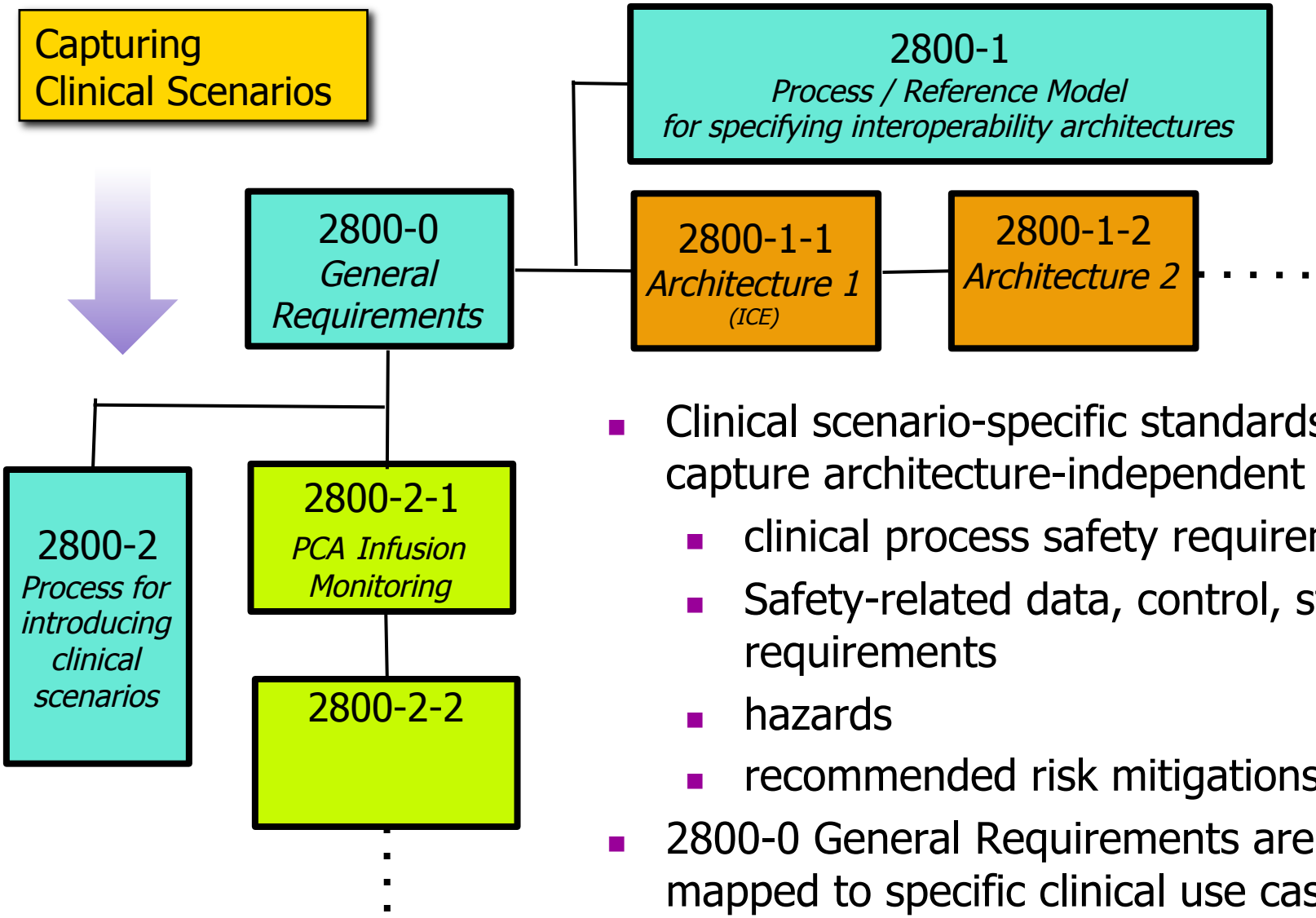
- Safety/Security and Essential Performance Objectives for interoperable systems
- Common vocabulary for referring to elements of interoperable systems
- General construction and architecture/interface specification requirements
- General risk management approach for interoperable systems
- Common fault types
- General requirements for testing, verification and establishing compliance
- General approach for compositional assurance case construction for interoperable systems

Proposed 2800 Structure



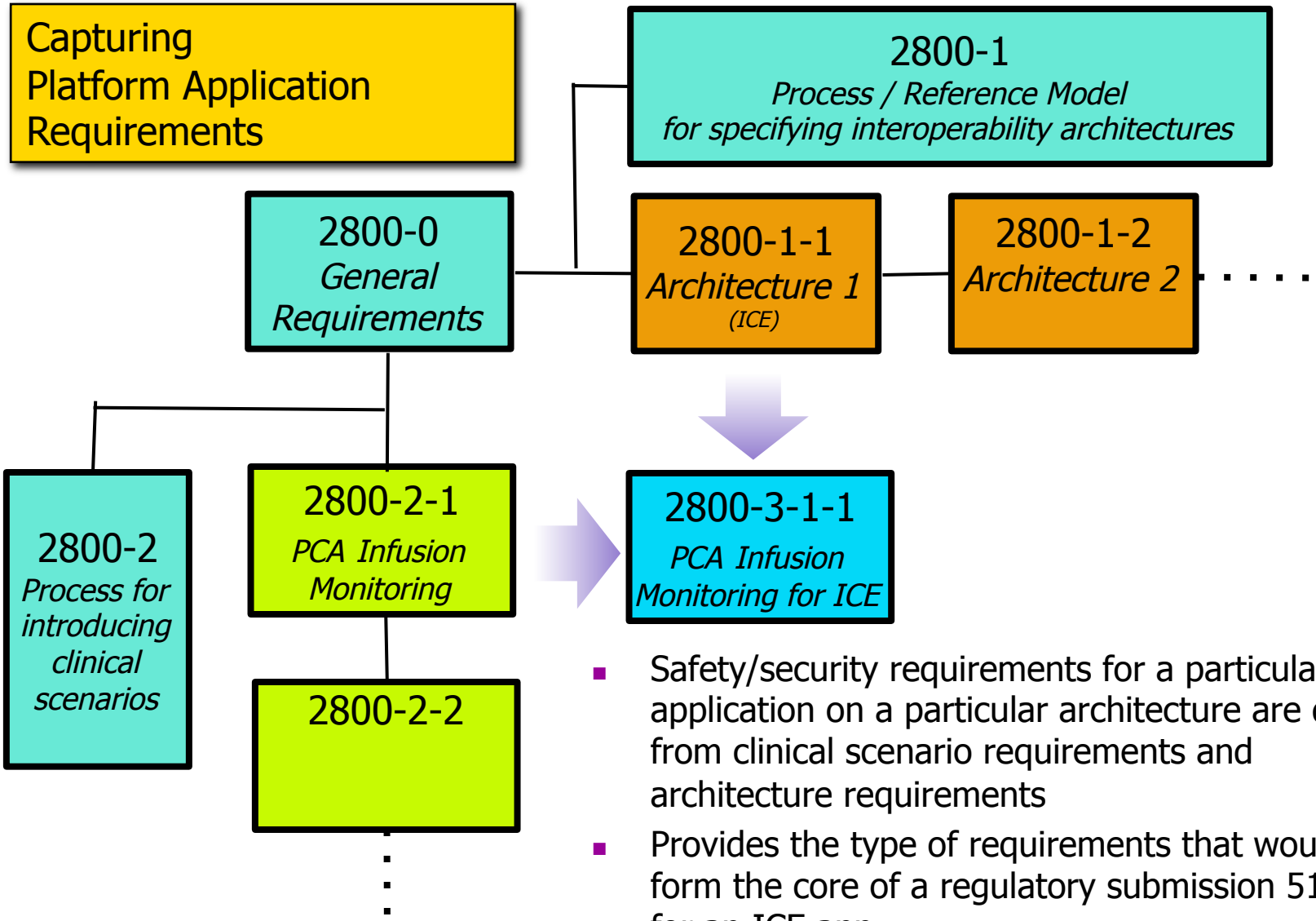
- Components assembled within 2800 is set up to allow specific architectures/ecospheres standards (2800-1-x) to be introduced, following guidelines for specifying interoperability architectures (2800-1)
- 2800-0 General Requirements are mapped to specific architectures and extended/refined

Proposed 2800 Structure



- Clinical scenario-specific standards capture architecture-independent
  - clinical process safety requirements
  - Safety-related data, control, state requirements
  - hazards
  - recommended risk mitigations
- 2800-0 General Requirements are mapped to specific clinical use cases

Proposed 2800 Structure



- Safety/security requirements for a particular application on a particular architecture are derived from clinical scenario requirements and architecture requirements
- Provides the type of requirements that would form the core of a regulatory submission 510(k) for an ICE app.

Leveraging Other Standards

2800 aims to leverage other work in the standards and interoperability spaces…

- IEC 61508: Functional Safety
- IEC 60601: Medical Safety
- ISO 14971: Medical Risk Management
- IEC 80001: Risk Management for IT Networks / Medical Devices
- IEEE 11073: Medical Device Interoperability
- IHE Profiles for semantic interoperability
- HL7 Standardization

The 61508 Association

HL7 HEALTH STANDARDS

ISO 14971:2009

IEC 60601-1 3rd Edition

ANSI/AAMI/ IEC 80001-1: 2010

IHE changing the way healthcare connects www.ihe.net

2800 Participants (excerpts)

- AAMI
- Anakena Solutions
- Baxter
- CIMIT (Mass General)
- Center for Medical Interoperability
- Continua Health Alliance
- DocBox
- Drexel University
- Draeger
- ECRI
- GE Medical
- Kansas State Univ.
- Medtronic
- NxStage Philips
- Smiths Medical
- Stryker
- Underwriters Laboratory
- Univ. of Pennsylvania
- US FDA
- US DoD (Veteran's Affairs)

Conclusions

- The MAP concept can…
  - enable rapid innovations in clinical system functionality
  - address safety issues that arise due to lack medical system integration.
- The technology exists to develop MAPs, but lack of architecture, interoperability, and relevant safety standards creates barriers to achieving the MAP vision
- Work such as ICE, 2800, etc. cannot provide "all the answers" at the moment, but it is aiming to
  - develop consensus around important architecture, safety/security, and ecosphere requirements
  - develop a path forward for address challenges
- Clinical engineers engineers will be called on to take a greater role in supporting interoperable systems and associated safety/security.
  - The MAP/2800 community needs input from clinical engineers to help identify important safety/security concerns to be addressed in MAP implementations and standards

Further Information…

ICE-Related Projects and Information…

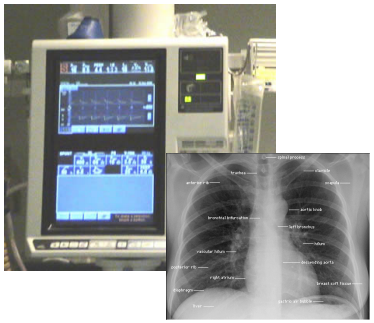
- CIMIT Medical Device Plug-and-Play Interoperability Project
  - http://www.mdpnp.org
- Medical Device Coordination Framework
  - http://mcdf.santos.ksu.edu
- DocBox
  - http://docboxinc.com
- Draeger Open SDC
  - http://sourceforge.net/projects/opensdc/

Extra Slides

Problematic Clinical Workflows

Example Use-Case: X-Ray / Ventilator Interaction

- Constant movement of a patient on ventilator makes it difficult to acquire x-ray image.
- Clinicians often manually disable ventilators -- sometimes with very bad consequences



A 32-year-old woman had a laparoscopic cholecystectomy [gall bladder removal] performed under general anesthesia. At the surgeons request, a plane film x-ray was shot during a cholangiogram [bile duct image]. The anesthesiologist stopped the ventilator for the film. The x-ray technician was unable to remove the film because of its position beneath the table. The anesthesiologist attempted to help her, but found it difficult because the gears on the table had jammed. Finally, the x-ray was removed, and the surgical procedure recommenced. At some point, the anesthesiologist glanced at the EKG and noticed severe bradycardia. He realized he had never restarted the ventilator. ***This patient ultimately expired****.*

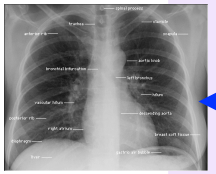
2005 Anesthesia Patient Safety Foundation Newsletter

Device Coordination

Fully leverage device data streams and the ability to *control* devices

Devices

***Moving forward**: live detection of patterns in monitoring data, automation of sequences of tasks in a clinical workflow*



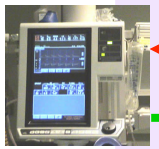
X-Ray Activation

Pause ventilator and activate x-ray when appropriate waveform point is signaled

Device Task controller

Confirmation Control

Anesthesiologist



Ventilator Pause Command

Breathing Pattern Data

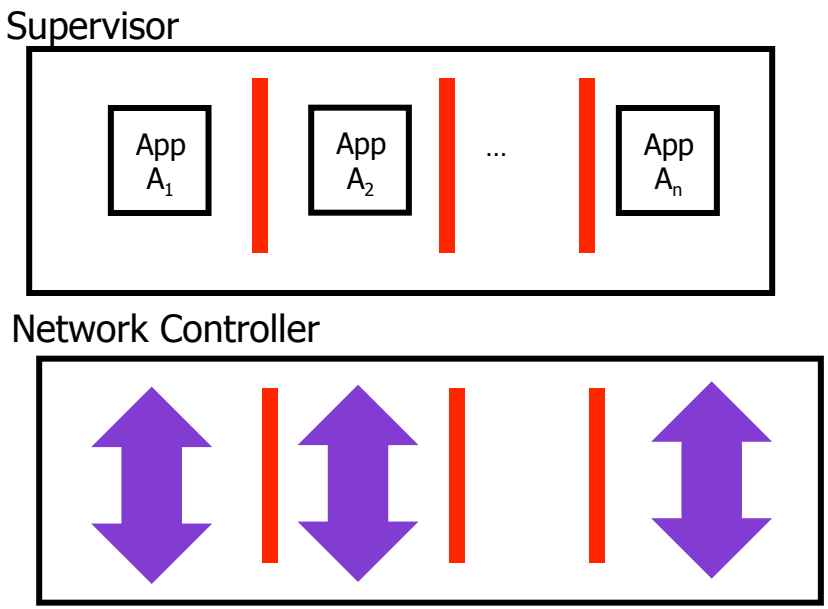
Single appropriate waveform point

Breathing Waveform Monitor

From Dr. Julian Goldman -- MDPnP.

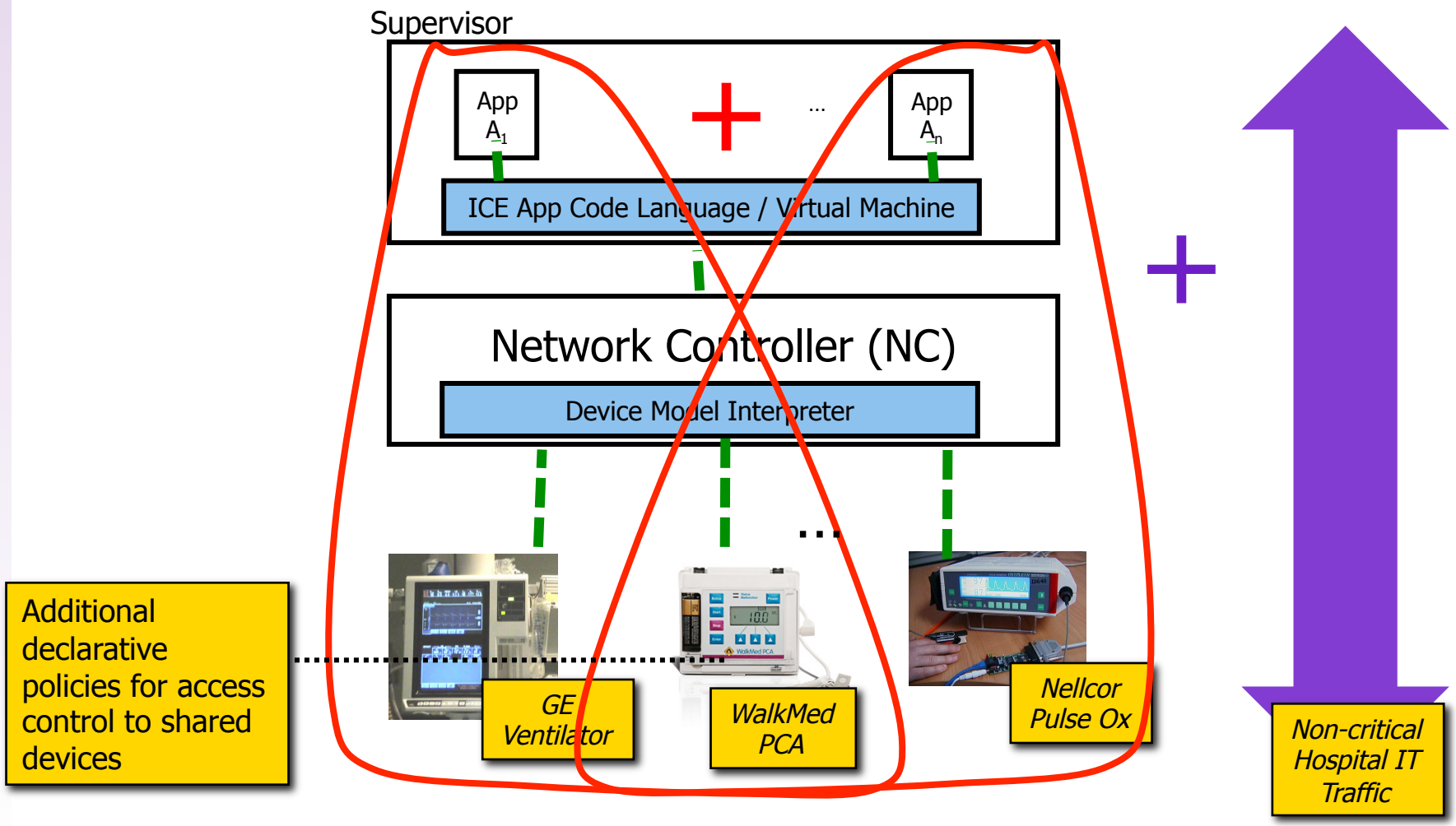
Key Partitioning Properties

A primary concept needed to support component-wise reasoning is *partitioning* – specifically, the platform/ architecture needs to provide guarantees that there *ALL* interactions between hosted resources are limited to explicitly declared interfaces. This allows us to reason about the safety, e.g., of one app without having to worry about the actions of another apps.



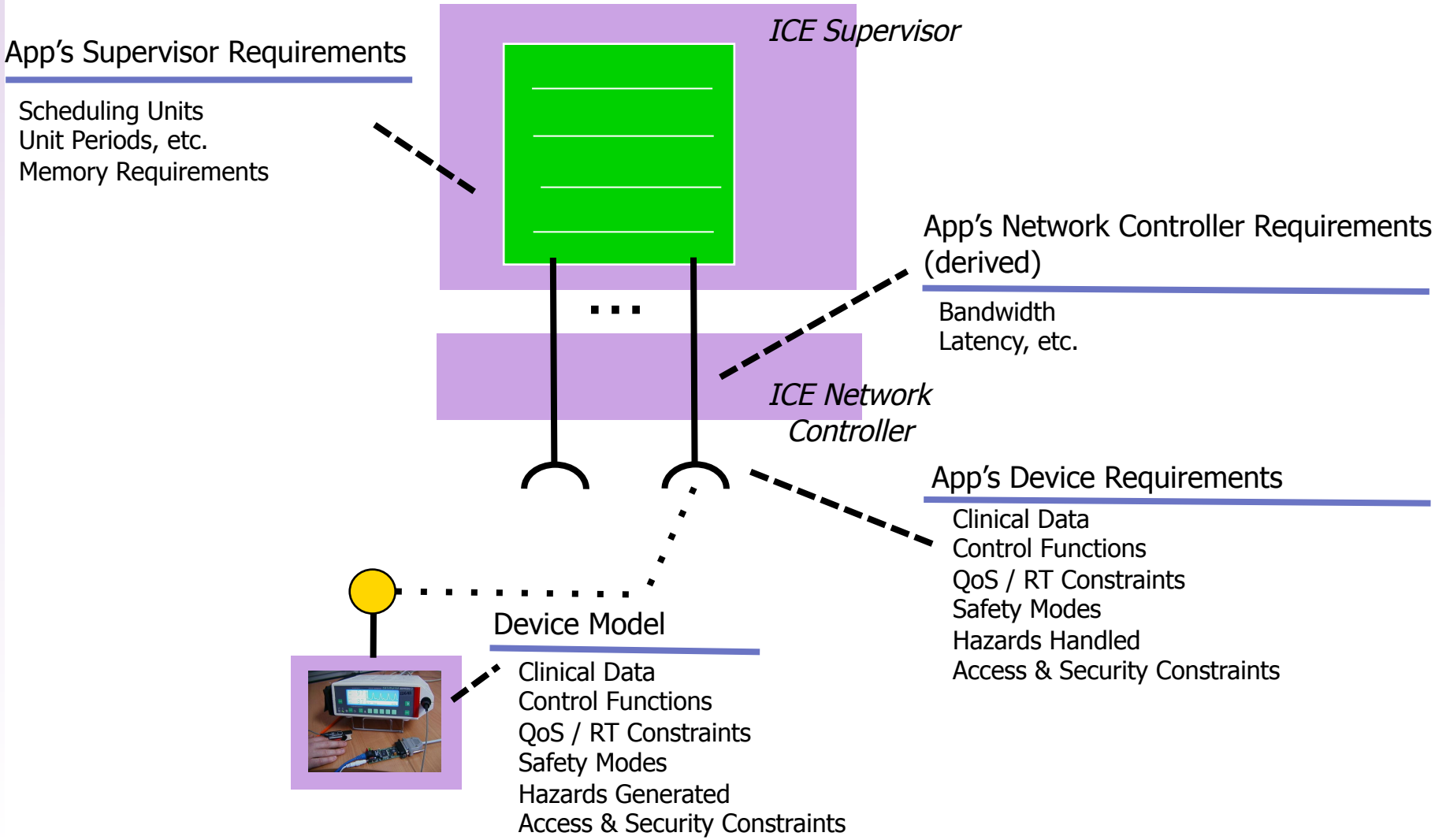
Partitioning enables Composition

Flexible / Dynamic partitioning provides foundations of non-interfering dynamic composition



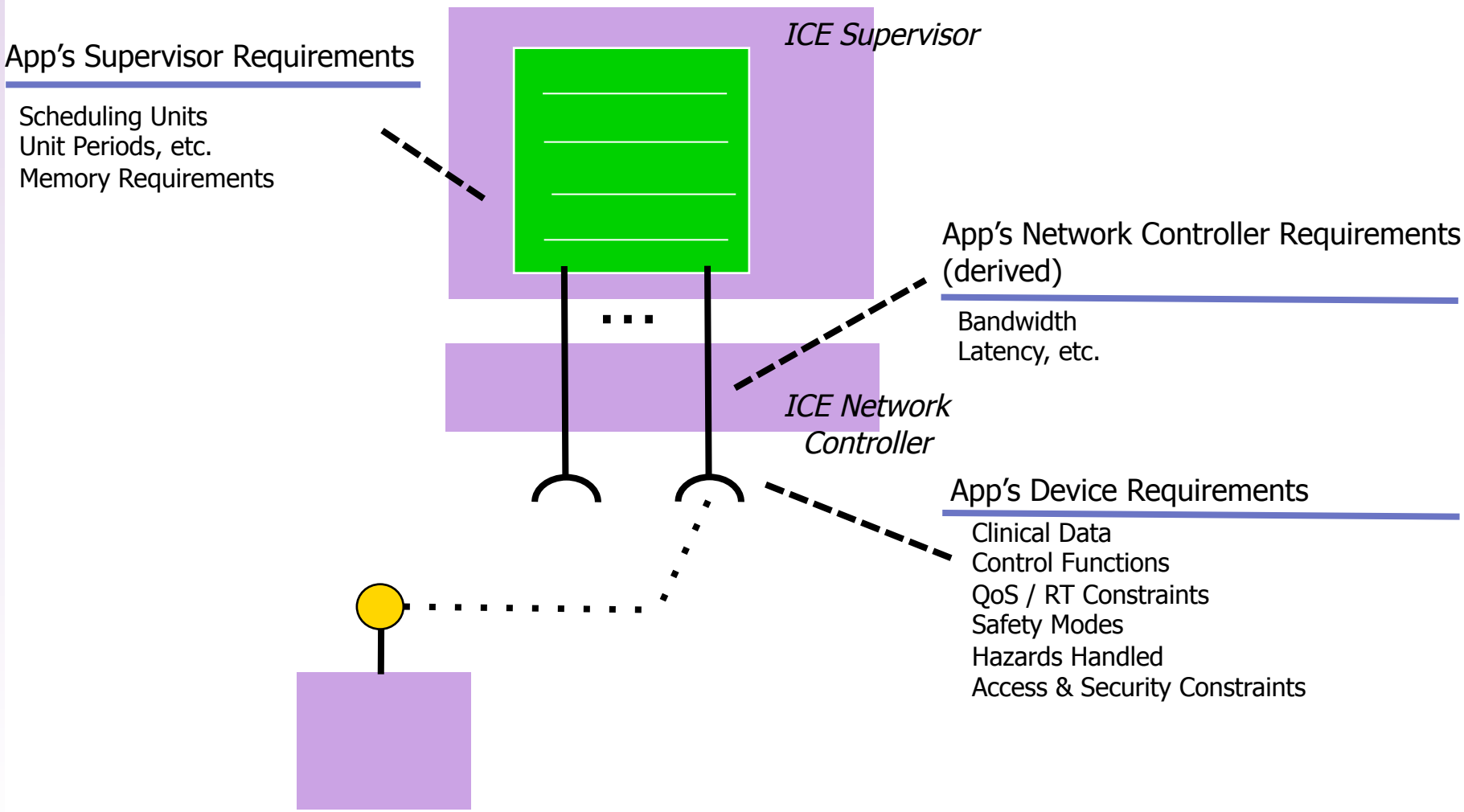
Apps Specify System Integration Aspects

Device declares its capabilities for supplying clinical data control functions, safety modes, QoS/RT properties. A priori third-party certification evaluates safety/correctness of device wrt those declarations.



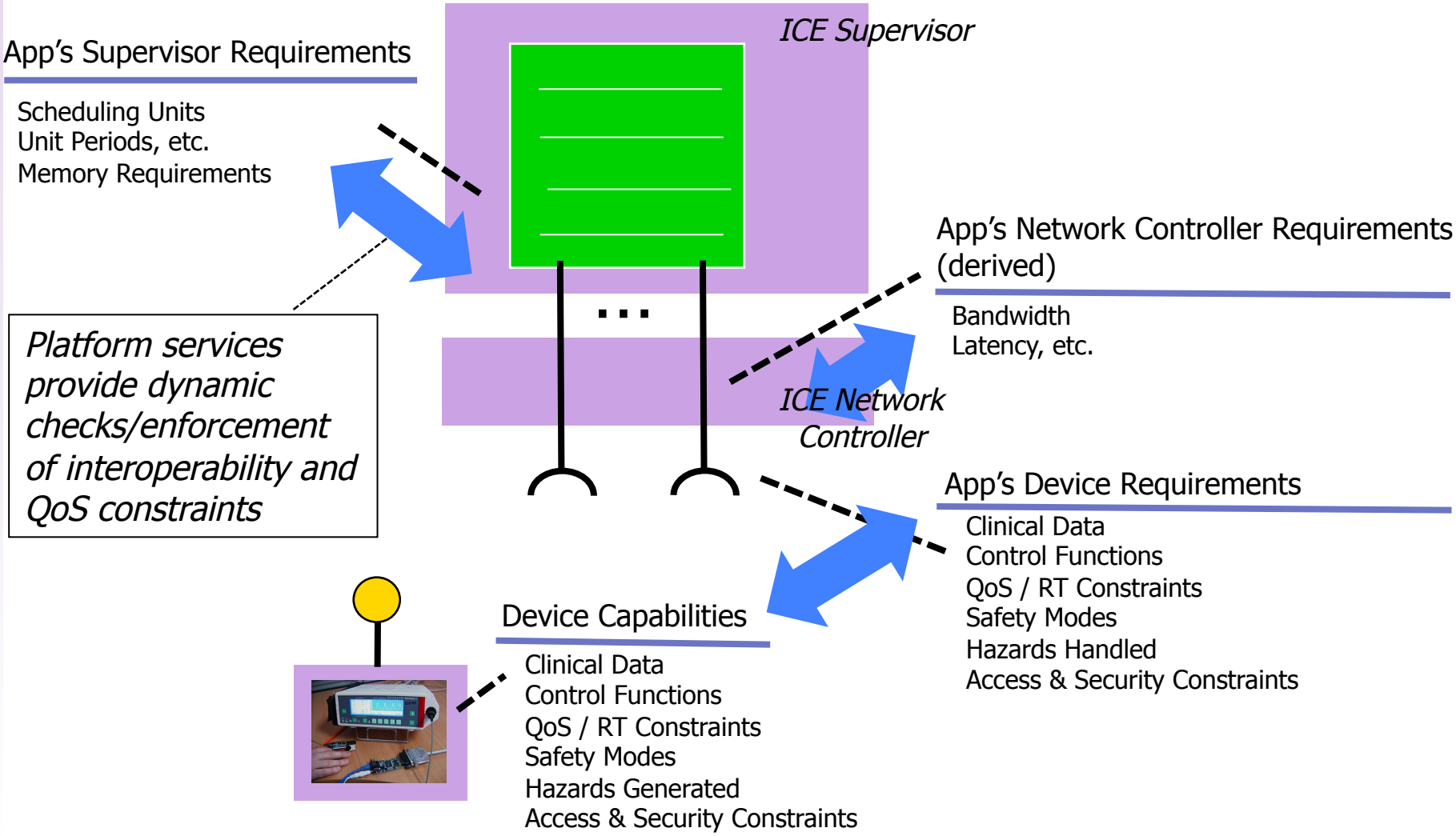
MDCF Apps Specify System Integration Aspects

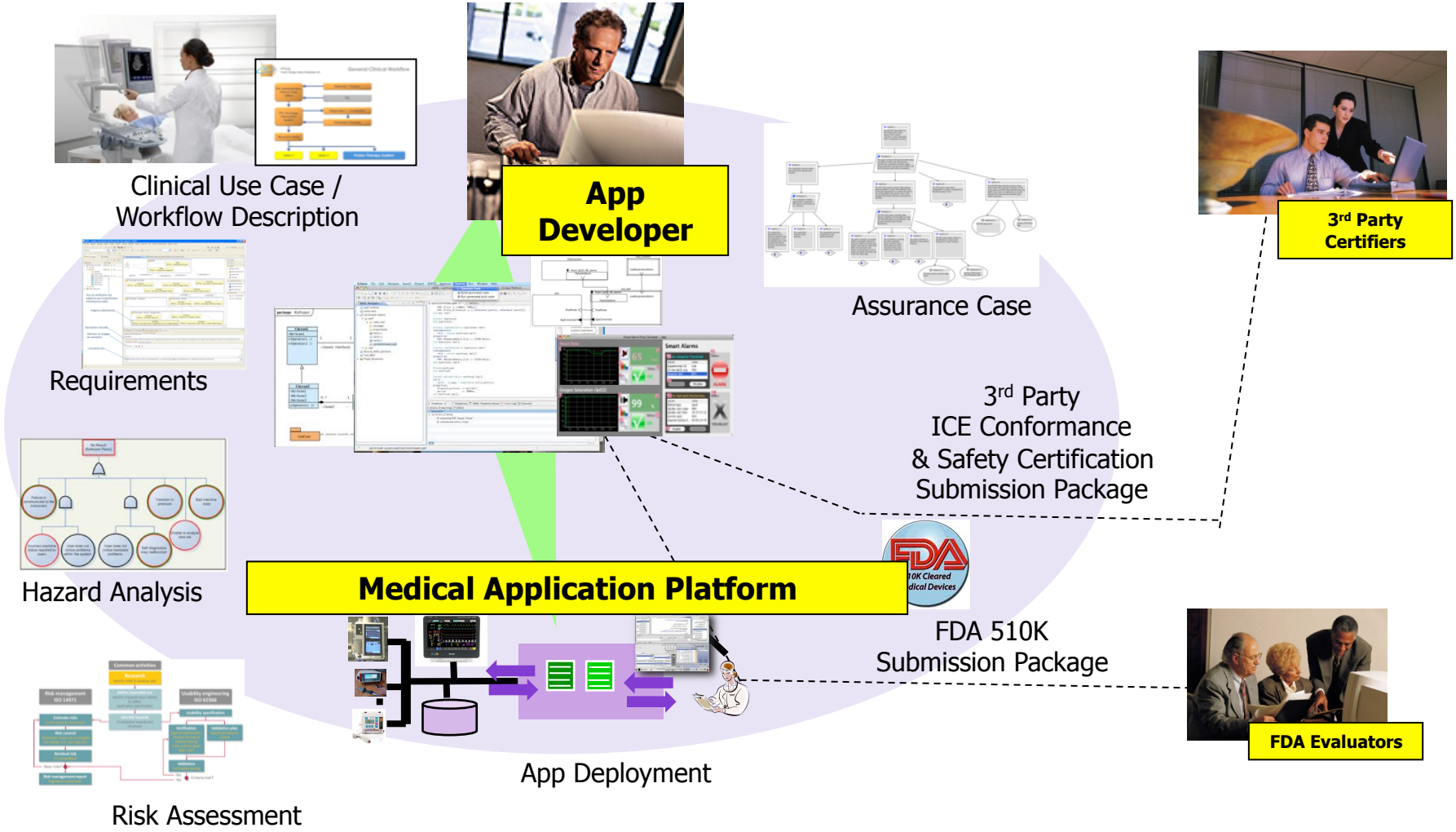
App declares its requirements for devices, communication, execution. A Priori third-Party certification evaluates safety/correctness of app wrt those declarations.



Trust via Staged Checking

At app launch time, platform services check to see whether platform and attached devices can satisfy requirements stated by the app. If so, app is launched. If not, app is not allowed to run.



Vision

Integrated Development and Verification Environment for ICE Apps