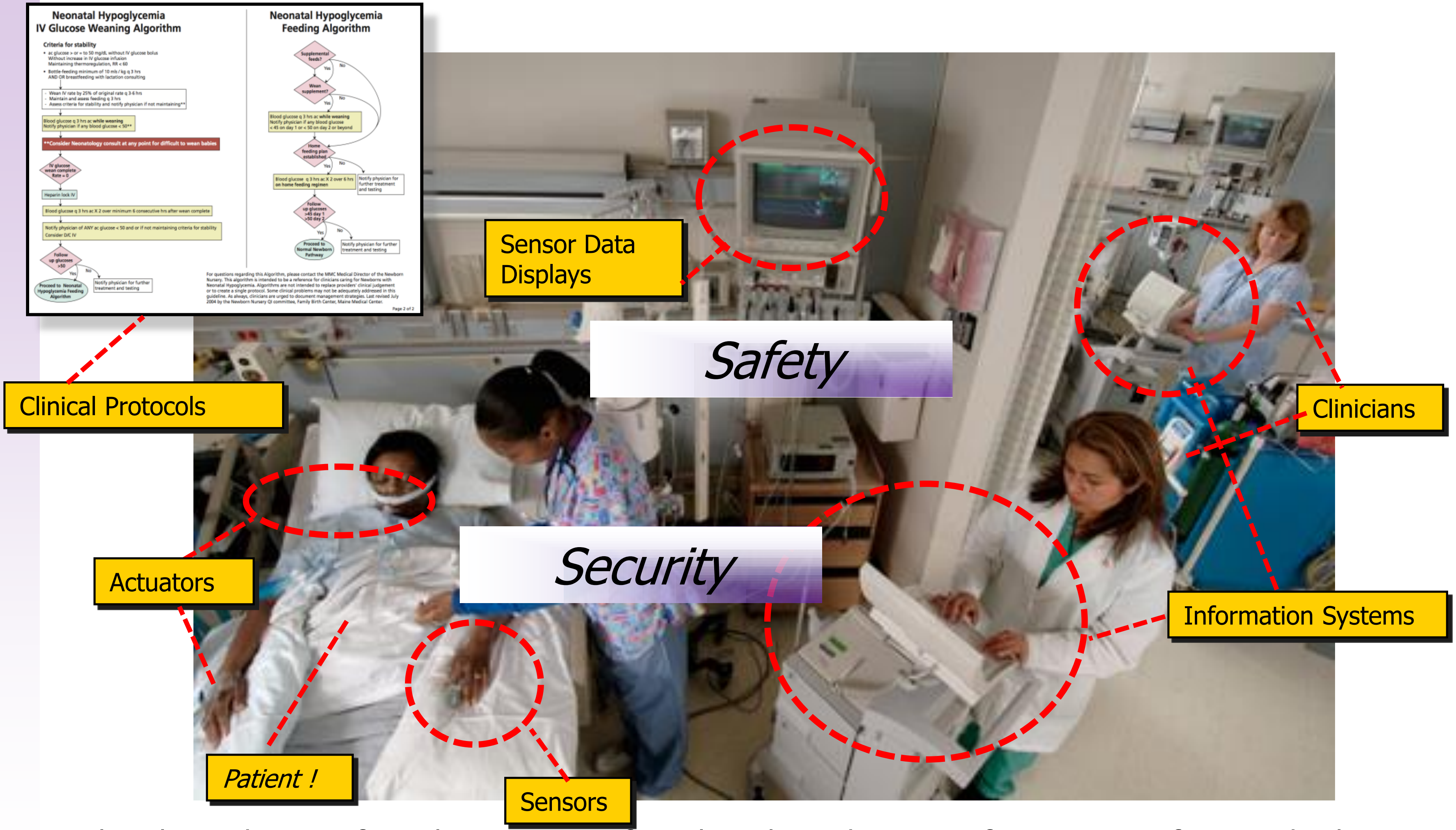
Challenges in Developing a Safety Standard for Medical Application Platforms

Anura Fernando – Underwriters Laboratories
John Hatcliff – Kansas State University

Support:

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

Health Care Involves
A Variety of System Components



Neonatal Hypoglycemia
IV Glucose Weaning Algorithm

Criteria for stability

- ac glucose > or = to 50 mg/dL without IV glucose bolus
  Without increase in IV glucose infusion
  Maintaining thermoregulation, RR < 60
- Bottle-feeding minimum of 10 mls / kg q 3 hrs
  AND OR breastfeeding with lactation consulting

- Wean IV rate by 25% of original rate q 3-6 hrs
- Maintain and assess feeding q 3 hrs
- Assess criteria for stability and notify physician if not maintaining**
Blood glucose q 3 hrs ac while weaning
Notify physician if any blood glucose < 50**
**Consider Neonatology consult at any point for difficult to wean babies
IV glucose wean complete Rate = 0
Heparin lock IV
Blood glucose q 3 hrs ac X 2 over minimum 6 consecutive hrs after wean complete
Notify physician of ANY ac glucose < 50 and or if not maintaining criteria for stability
Consider D/C IV
Follow up glucoses >50
Yes
No
Proceed to Neonatal Hypoglycemia Feeding Algorithm
Notify physician for further treatment and testing

Neonatal Hypoglycemia
Feeding Algorithm

Supplemental feeds?
Yes
No
Wean supplement?
Yes
No
Blood glucose q 3 hrs ac while weaning
Notify physician if any blood glucose
< 45 on day 1 or < 50 on day 2 or beyond
Home feeding plan established
Yes
No
Blood glucose q 3 hrs ac X 2 over 6 hrs on home feeding regimen
Notify physician for further treatment and testing
Follow up glucoses >45 day 1 >50 day 2
Yes
No
Proceed to Normal Newborn Pathway
Notify physician for further treatment and testing

For questions regarding this Algorithm, please contact the MMC Medical Director of the Newborn Nursery. This algorithm is intended to be a reference for clinicians caring for Newborns with Neonatal Hypoglycemia. Algorithms are not intended to replace providers' clinical judgement or to create a single protocol. Some clinical problems may not be adequately addressed in this guideline. As always, clinicians are urged to document management strategies. Last revised July 2004 by the Newborn Nursery QI committee, Family Birth Center, Maine Medical Center.

Page 2 of 2

Sensor Data Displays

Safety

Clinical Protocols

Clinicians

Actuators

Security

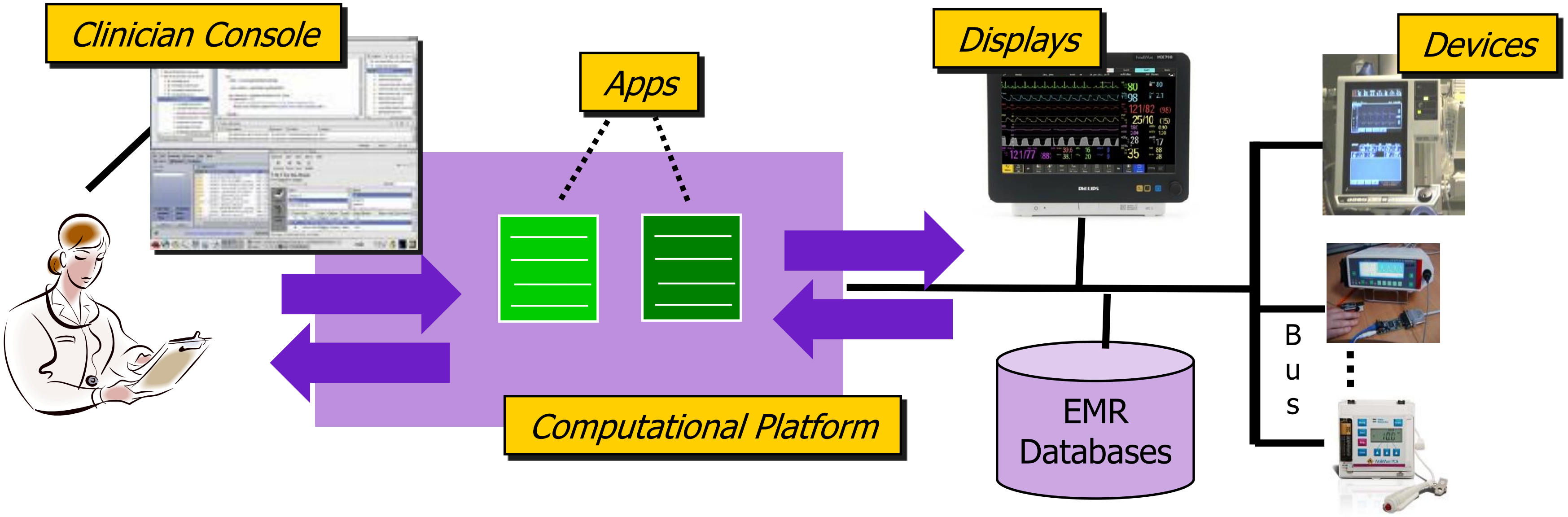
Information Systems

Patient !

Sensors

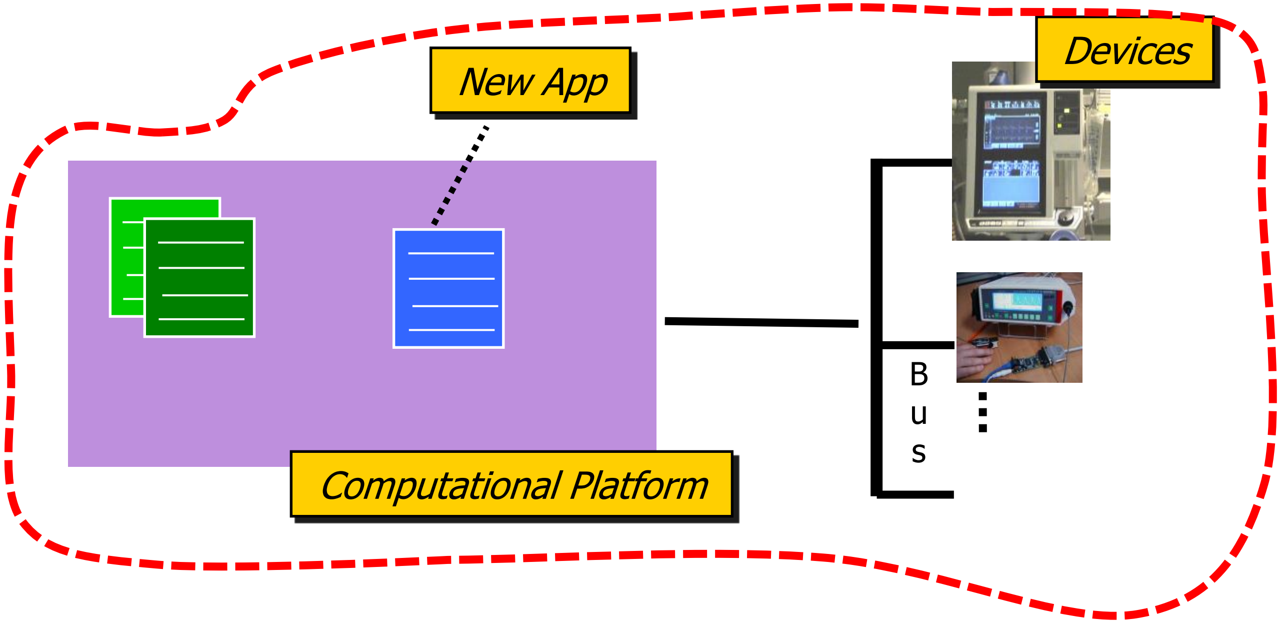
Together these elements form the precursor of a Cyber-Physical System of Systems. Unfortunately, these elements are largely un-integrated, and so appropriate automated systems solutions cannot be applied.

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

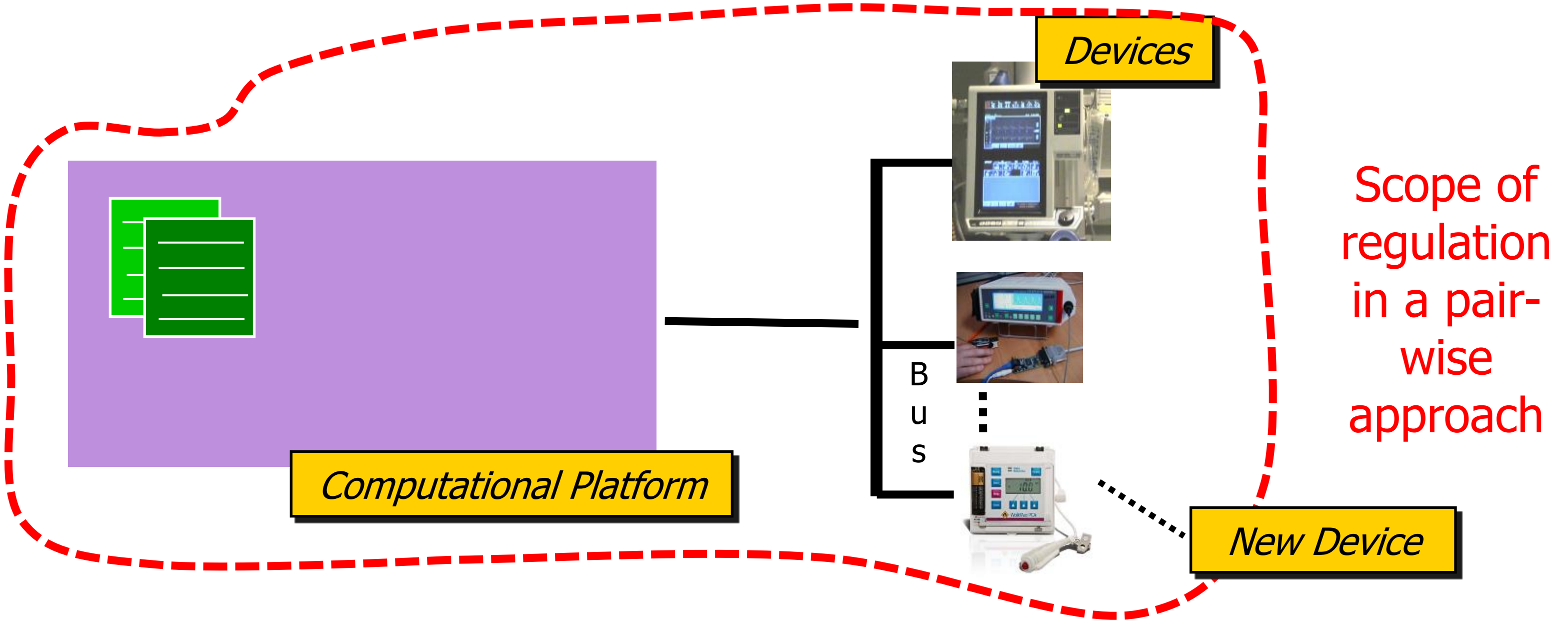
Needed: New Regulatory Approach



Scope of regulation in a pair-wise approach

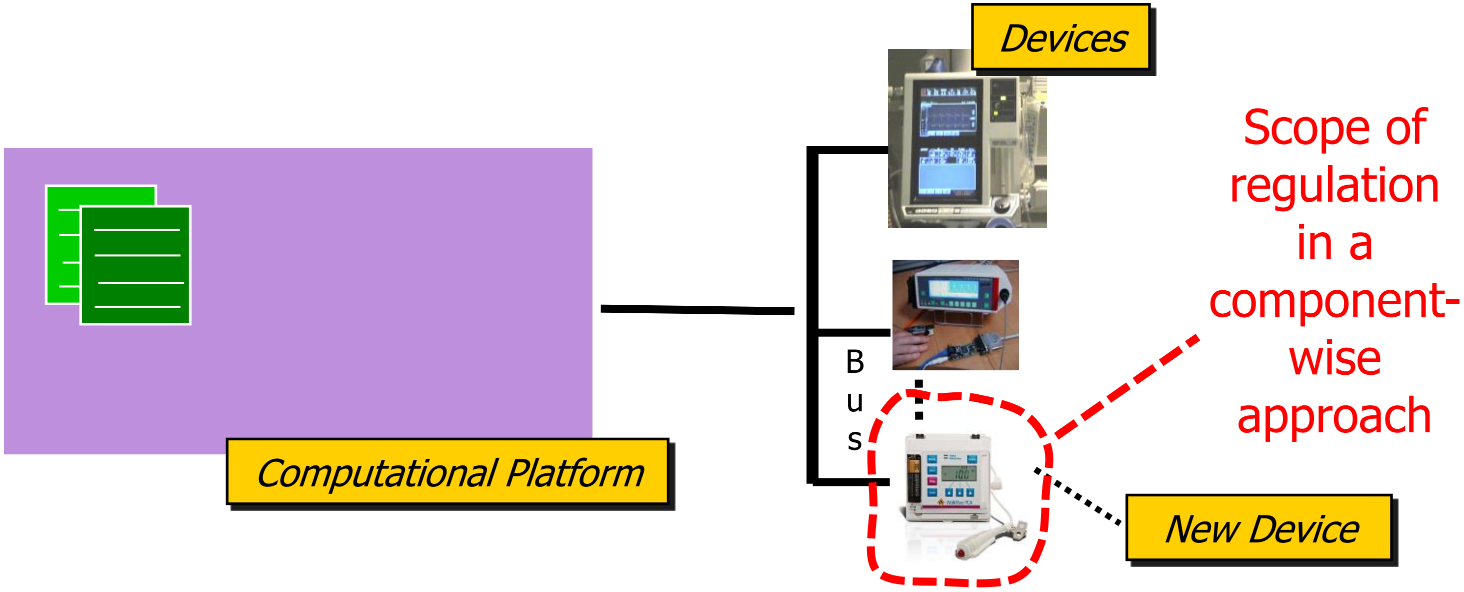
- In the current “pair-wise” certification/regulatory approach, when adding a new app…
  - …the scope of regulation would be the entire system
  - …i.e., set of all MAP instances and app would need to be submitted for regulatory approval

Needed: New Regulatory Approach



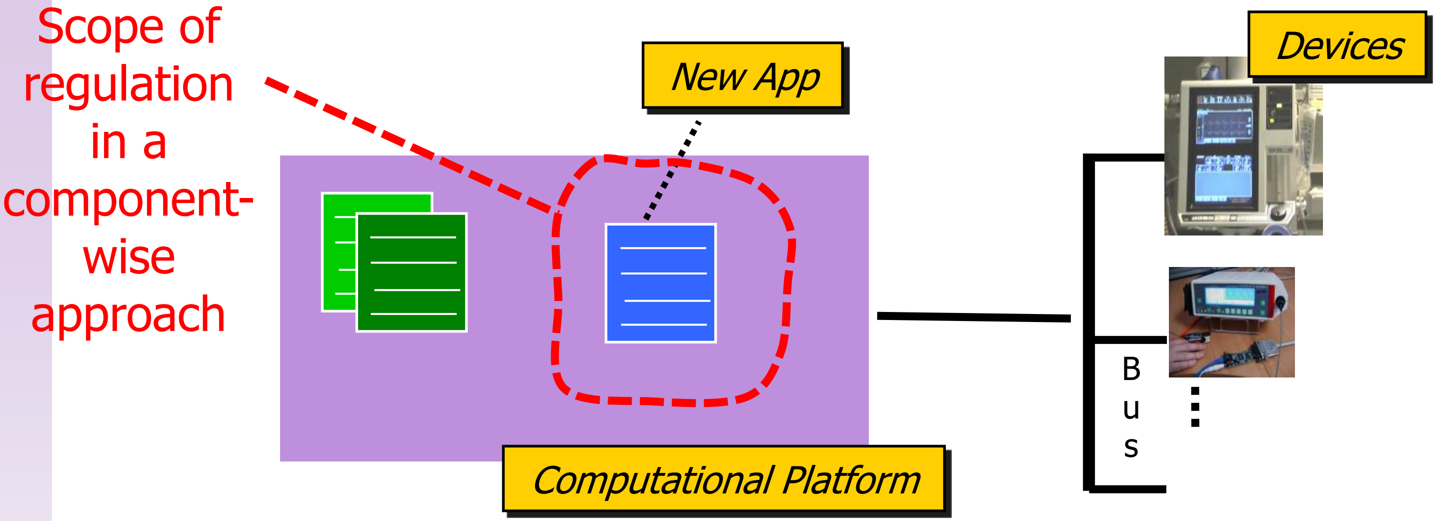
- In the current "pair-wise" certification/regulatory approach, when adding a new device…
  - …the scope of regulation would be the entire system
  - …i.e., set of all MAP instances and device would need to be submitted for regulatory approval

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, hazards, safety-states?
    - Does it appropriately implement the MAP networking protocols?

Envisioned Compositional Approach

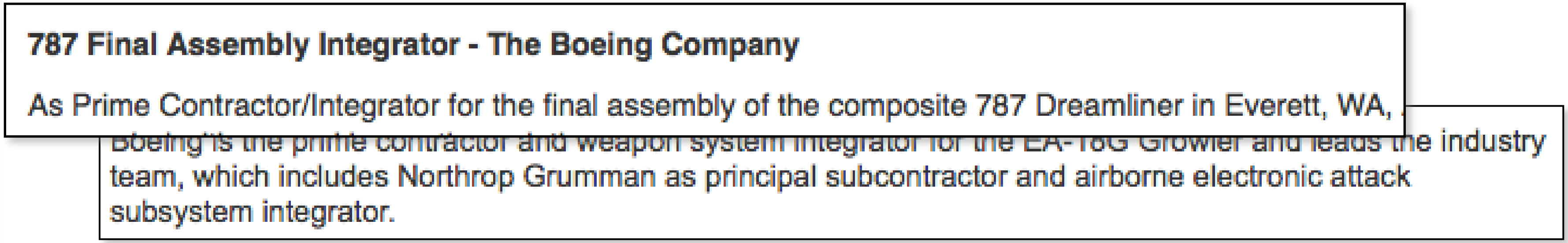


- In an envisioned “component-wise” regulatory approach, when adding a new app…
  - …the scope of regulation would be the just the app
  - …the app specifies its requirements for devices and platform capabilities (which would be checked by the platform at launch time)
  - …the app regulatory submission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

System Integration

In other safety critical domains, there is a typically a prime contractor that is responsible for integration and system-level verification and validation.

- Integration is performed *before* deployment with full knowledge and behavior of components being integrated
- Integrator has expert-level technical knowledge of components & system behavior
- Responsible for overall system
  - Verification & Validation
  - Safety arguments
  - Certification



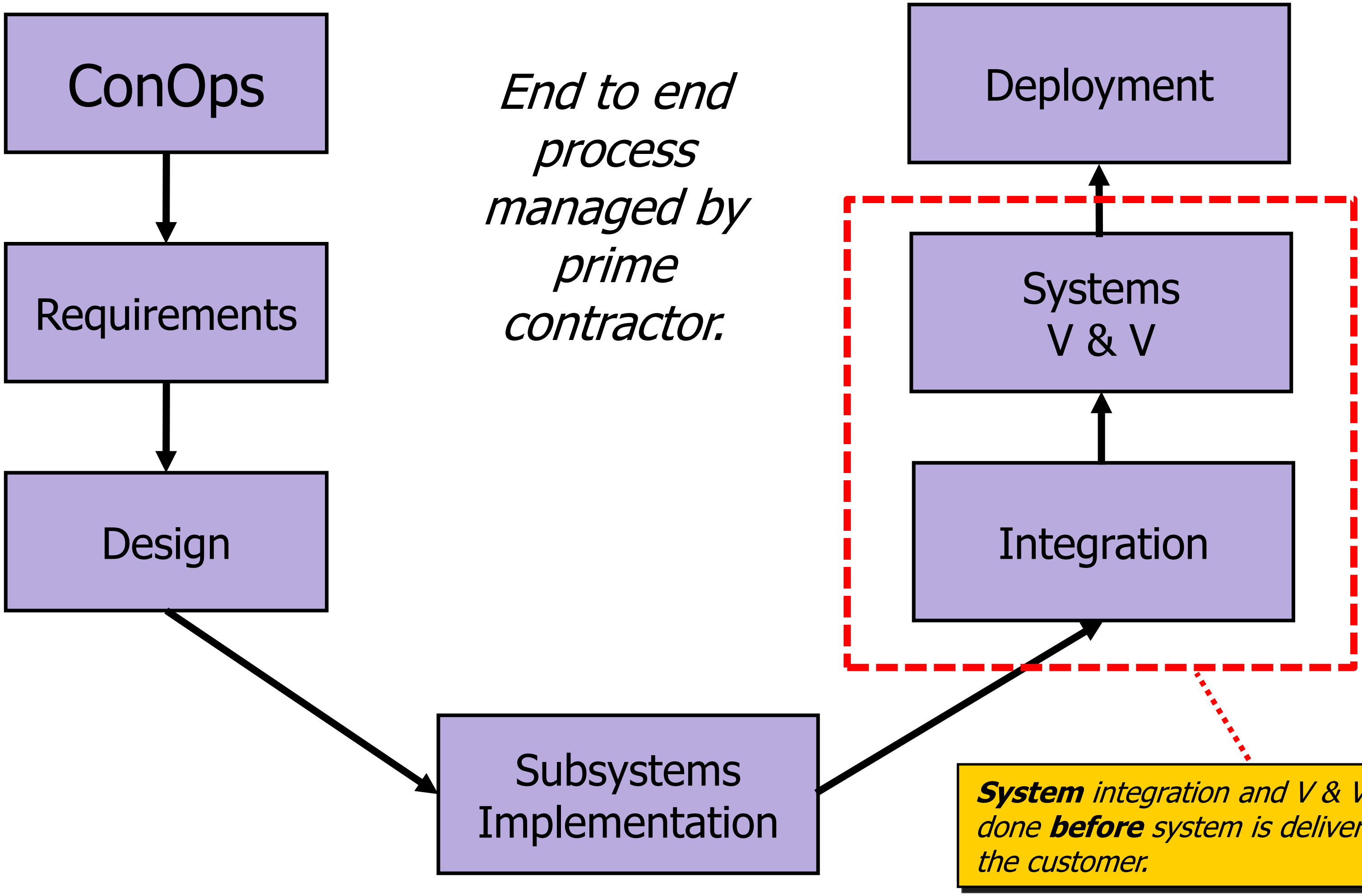
787 Final Assembly Integrator - The Boeing Company

As Prime Contractor/Integrator for the final assembly of the composite 787 Dreamliner in Everett, WA,

Boeing is the prime contractor and weapon system integrator for the EA-18G Growler and leads the industry team, which includes Northrop Grumman as principal subcontractor and airborne electronic attack subsystem integrator.

System Integration

In other safety critical domains, there is a typically a prime contractor that is responsible for integration and system-level verification and validation.



ConOps

Requirements

Design

Subsystems Implementation

Integration

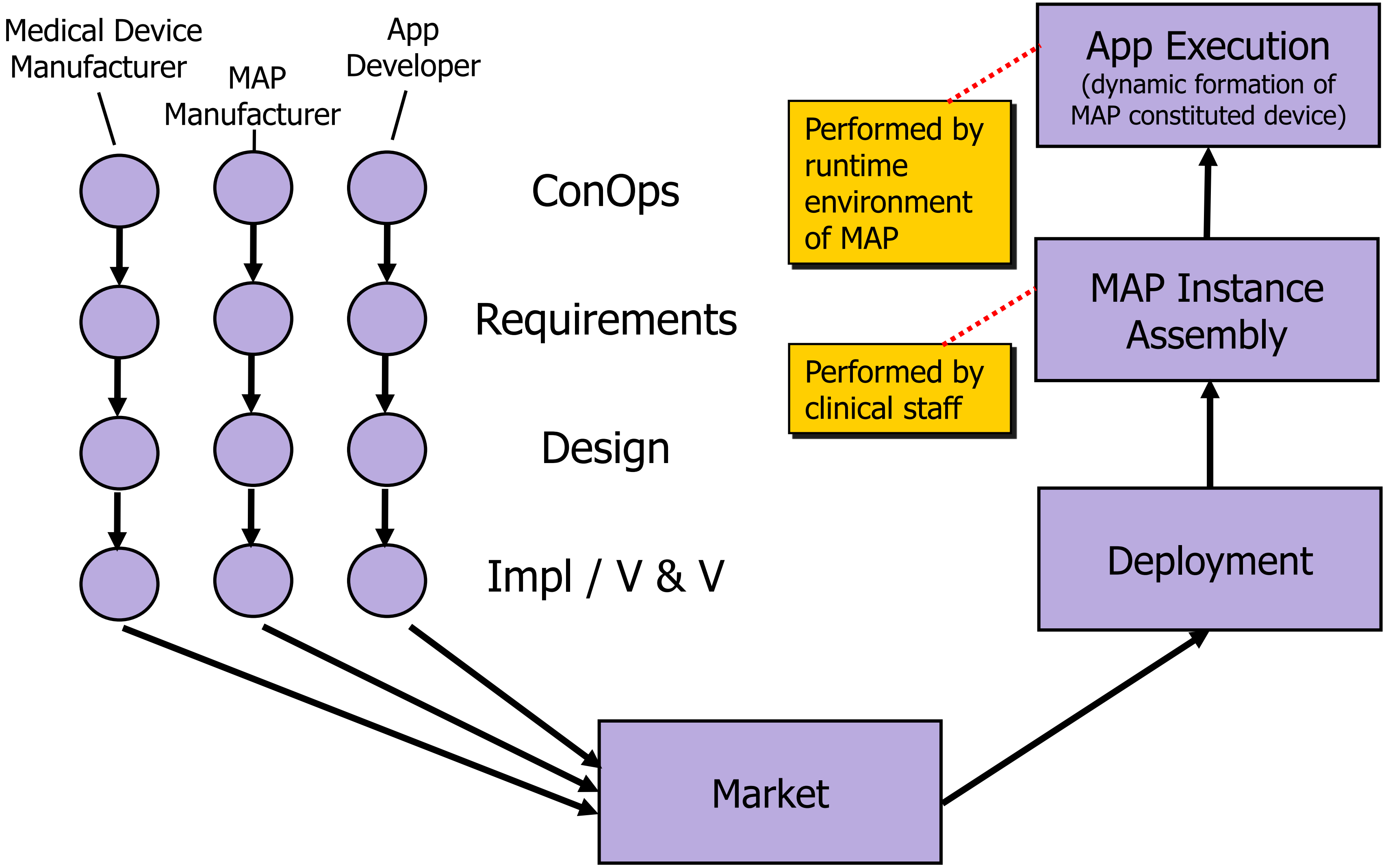
Systems V & V

Deployment

End to end process managed by prime contractor.

System *integration and V & V is done* ***before*** *system is delivered to the customer.*

MAP Development & Assembly


Medical Device Manufacturer
MAP Manufacturer
App Developer
ConOps
Requirements
Design
Impl / V & V
Market
Deployment
MAP Instance Assembly
App Execution
(dynamic formation of MAP constituted device)
Performed by runtime environment of MAP
Performed by clinical staff

MAP Characteristics

In other safety critical domains, there is a typically a prime contractor that is responsible for integration and system-level verification and validation.

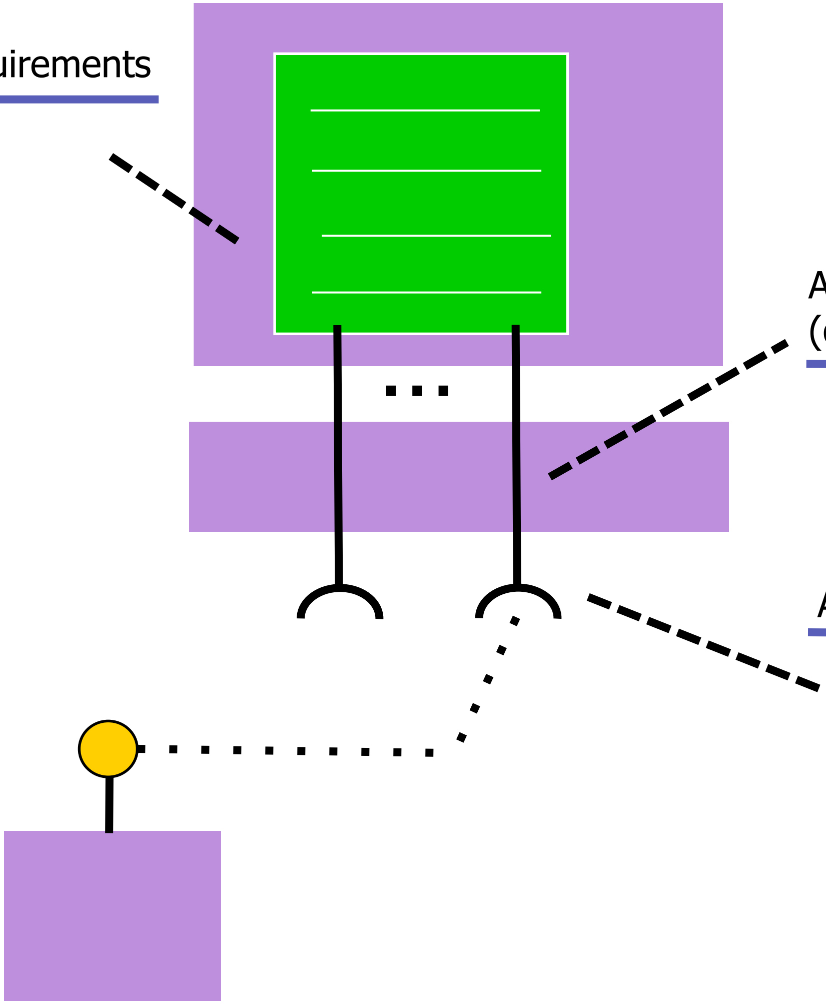
- Integration is performed *before* deployment with full knowledge and behavior of components being integrated
- Integrator has expert-level technical knowledge of components & system behavior
- Responsible for overall system
  - Verification & Validation
  - Safety arguments
  - Certification

With MAPs, there is **no** prime contractor that is responsible for integration and system-level verification and validation.

- Assembly is performed *after* deployment
- Assembler (hospital staff) **does not have** expert-level technical knowledge of components & system behavior
- **App developer** is responsible for overall
  - System safety arguments
- Platform services (compatibility checks) assist in determining **at app launch time** if platform and attached devices satisfy requirements of app
- The app's directions for assembly of the platform constituted device are stated **only in terms of properties/capabilities that are exposed on the interfaces** of the platform and devices.

Trust via Staged Checking

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



App's Supervisor Requirements

Scheduling Units
Unit Periods, etc.
Memory Requirements

App's Network Controller Requirements (derived)

Bandwidth
Latency, etc.

App's Device Requirements

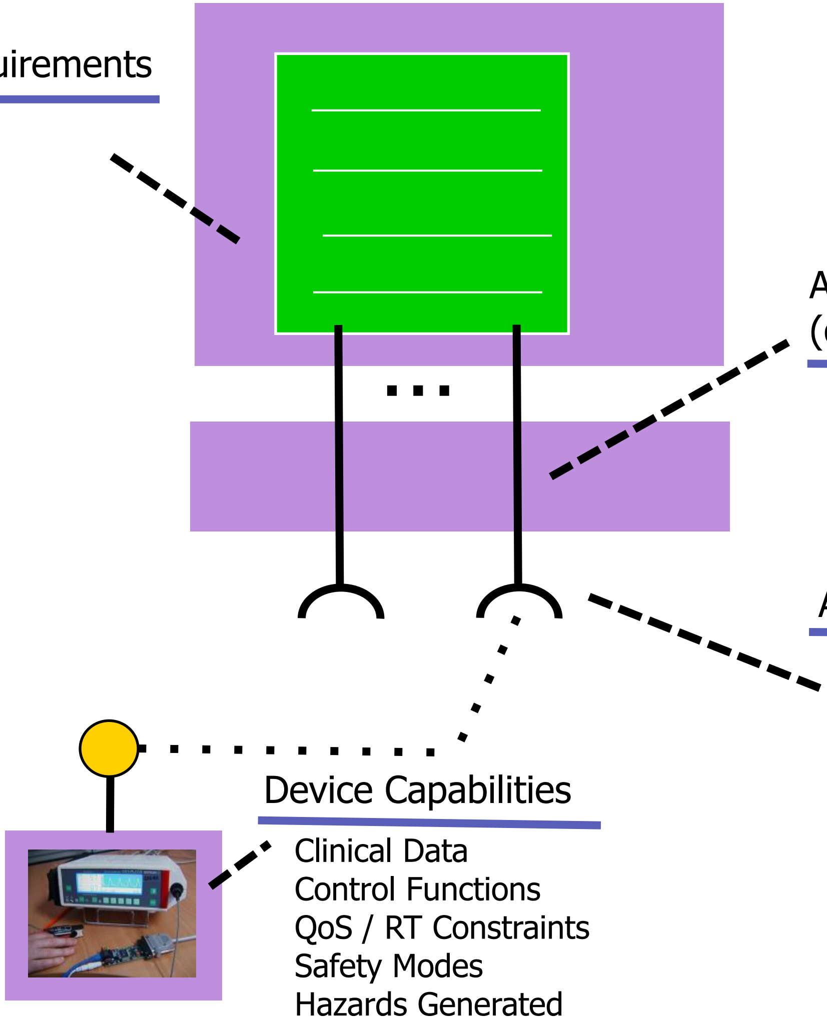
Clinical Data
Control Functions
QoS / RT Constraints
Safety Modes
Hazards Handled
Access & Security Constraints

Trust via Staged Checking

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.

App's Supervisor Requirements

Scheduling Units
Unit Periods, etc.
Memory Requirements



App's Network Controller Requirements (derived)

Bandwidth
Latency, etc.

App's Device Requirements

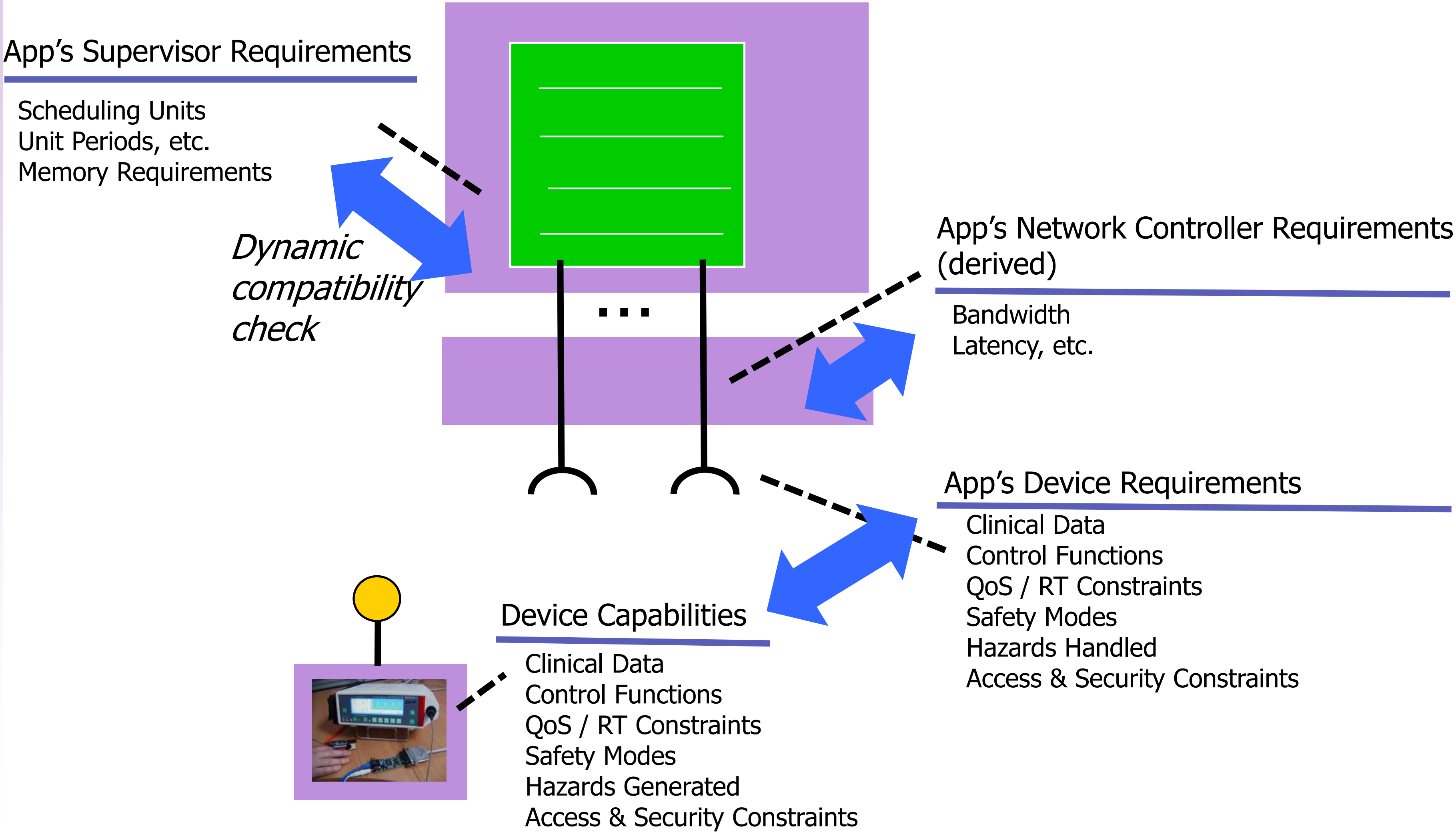
Clinical Data
Control Functions
QoS / RT Constraints
Safety Modes
Hazards Handled
Access & Security Constraints

Device Capabilities

Clinical Data
Control Functions
QoS / RT Constraints
Safety Modes
Hazards Generated
Access & Security Constraints

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.



App's Supervisor Requirements

Scheduling Units
Unit Periods, etc.
Memory Requirements

Dynamic compatibility check

App's Network Controller Requirements (derived)

Bandwidth
Latency, etc.

App's Device Requirements

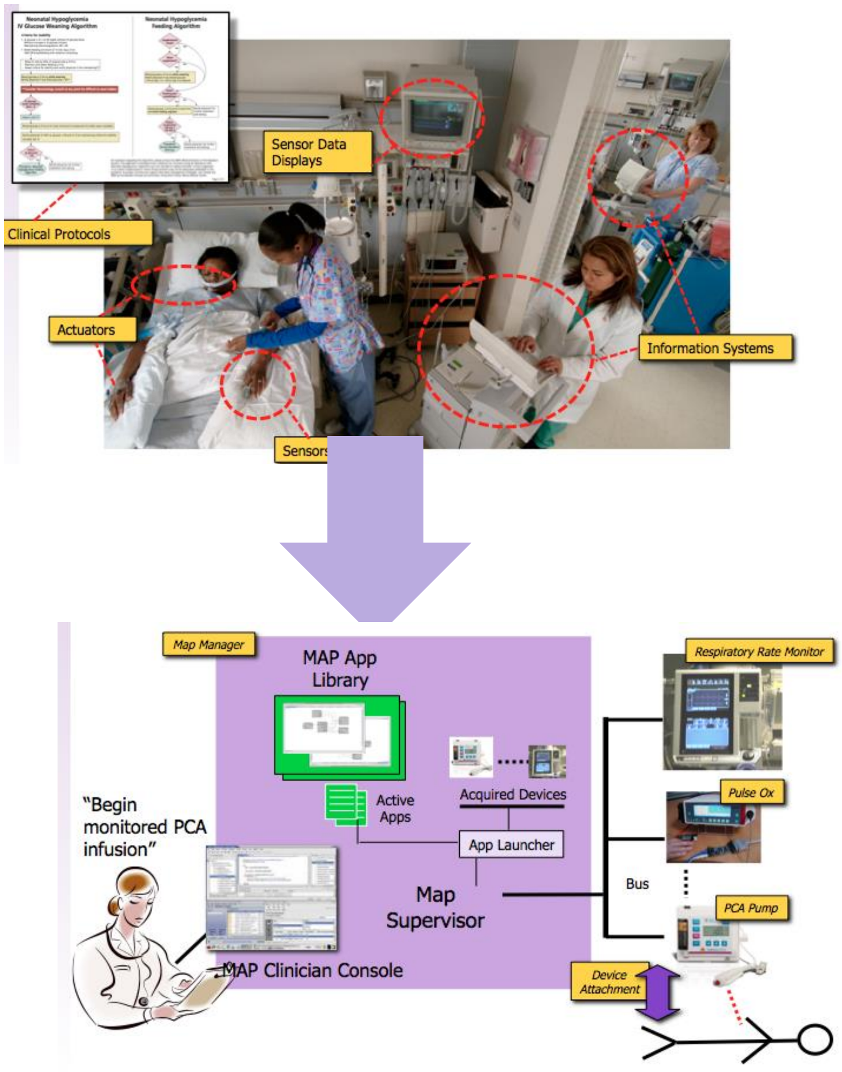
Clinical Data
Control Functions
QoS / RT Constraints
Safety Modes
Hazards Handled
Access & Security Constraints

Device Capabilities

Clinical Data
Control Functions
QoS / RT Constraints
Safety Modes
Hazards Generated
Access & Security Constraints

How to Achieve the MAP Vision?

- A rigorous architecture oriented to compositional safety/trust
- Precise/formal interface specifications capturing a variety of properties
  - Including real-time and resource constraints
- *Static Enforcement* -- Formal verification techniques for checking interface compatibility and implementation compliance to interfaces
- *Dynamic Enforcement* -- Run-time enforcement that app's requirements on platform and devices are satisfied
- Rigorous third-party certification of compliance to architecture/interfaces



KSU / UL Collaboration

Open experimental ICE-compliant platform to bring together academic researchers, industry vendors, and government regulators

- UL / AAMI have formed a Joint Committee on Medical Device Interoperability
  - goal is to create a family of *safety standards* for medical application platforms
- KSU is providing inputs based on experience with the *Medical Device Coordination Framework* – prototype MAP environment
  - Developed by Kansas State University and U Penn
  - Funded by NSF CPS and NSF FDA Scholar-in-Residence programs
- Focus of KSU/UL Interactions
  - Formal architecture descriptions in AADL
  - Tool-supported risk management based on the AADL Error Model annex
  - Using the PCA artifacts described in the afternoon sessions as case studies

Medical Device Coordination Framework

Open experimental ICE-compliant platform to bring together academic researchers, industry vendors, and government regulators

- Background
  - Developed by Kansas State University and U Penn
  - Funded by NSF CPS and NSF FDA Scholar-in-Residence programs
- Goals
  - Open source infrastructure
  - Meet performance requirements of realistic clinical scenarios
  - Provide middleware with reliability, real-time, security
  - Provide an effective app programming model and development environment with integrated verification/validation support and construction of regulatory artifacts
  - Support evaluation of device interfacing concepts
  - Illustrate how to support real and mock devices
  - Illustrate envisioned regulatory oversight and 3rd party certification