Challenges in Medical CPS

Oleg Sokolsky

PRECISE Center

University of Pennsylvania

PERSYVAL-Lab Summer School on CPS

July 10, 2013

Penn Engineering

PRECISE

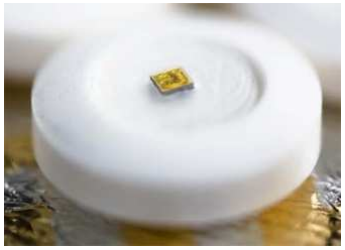
Outline

- Trends in Medical CPS
- Stand-alone devices
  - Pacemaker
  - Infusion Pump
- Medical device interoperability
  - Promises and challenges
  - IEEE/ISO 11073 standard
  - Clinical scenarios as virtual devices
  - Physiological Closed-loop Systems

Trends in Medical Cyber-Physical Systems (MCPS)

Miniaturization

- Implantable devices
- Ingestible sensors



Interoperation

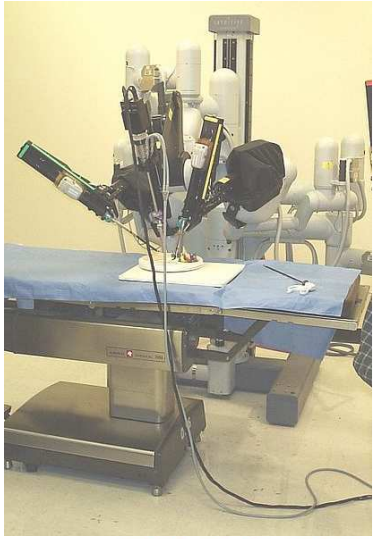
- Executable clinical scenarios
- Safety interlocks

Teleoperation

- Tele-ICU
- Robotic surgery

Autonomy

- Smart alarms
- Context-sensitive decision support
- Physiological closed loop control



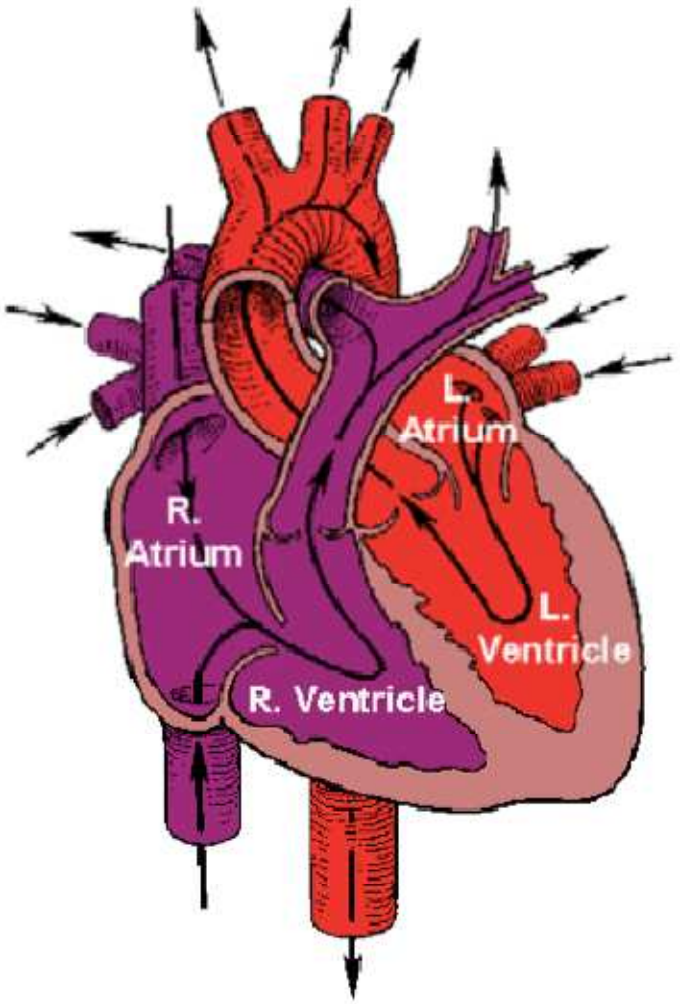
Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Outline

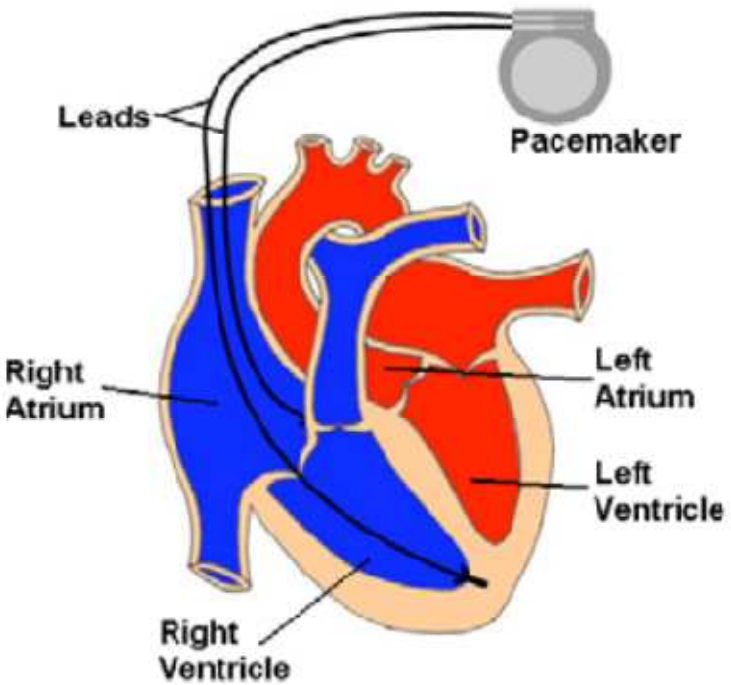
- Trends in Medical CPS
- Stand-alone devices
  - Pacemaker
  - Infusion Pump
- Medical device interoperability
  - Promises and challenges
  - IEEE/ISO 11073 standard
  - Clinical scenarios as virtual devices
  - Physiological Closed-loop Systems

Background: The human heart



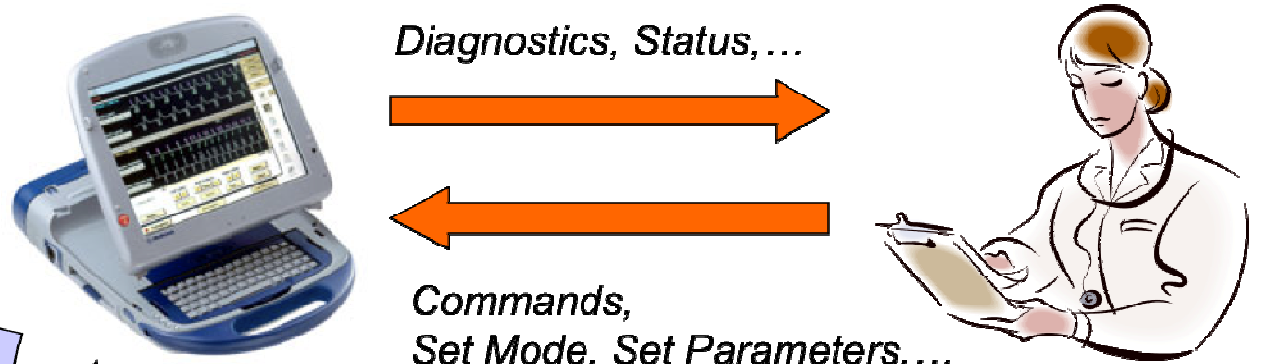
- Four chambers: atria & ventricles
- Electrical stimulus in the right atrium
  - heart's chambers contract & pump blood into ventricles
  - the ventricles pump blood into arteries
- When this system does not work properly, a pacemaker may be used to regulate the heart rate

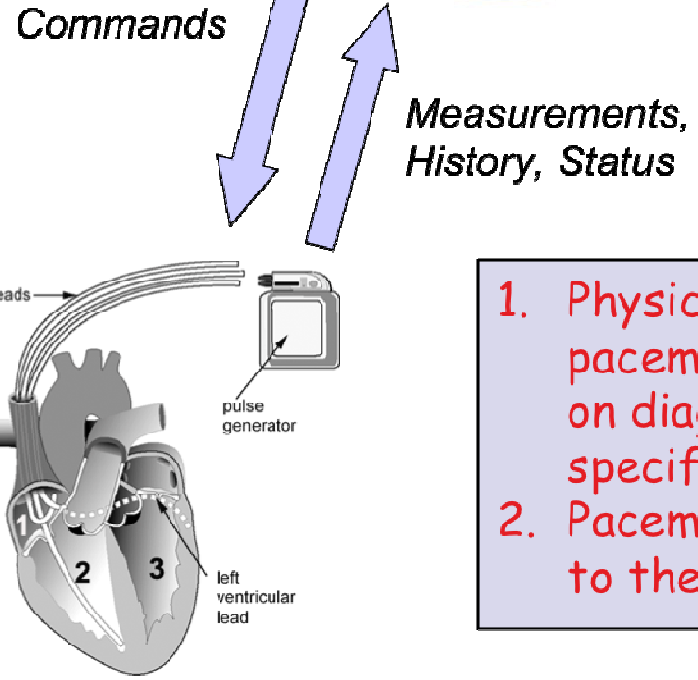
Cardiac Pacemaker



- Deliver electrical stimuli, or paces, over leads with electrodes that are in contact with the heart
- May detect natural cardiac stimulations, called senses
- Requirements for the pacemaker are given in terms of timing cycles

Programming vs. Operation

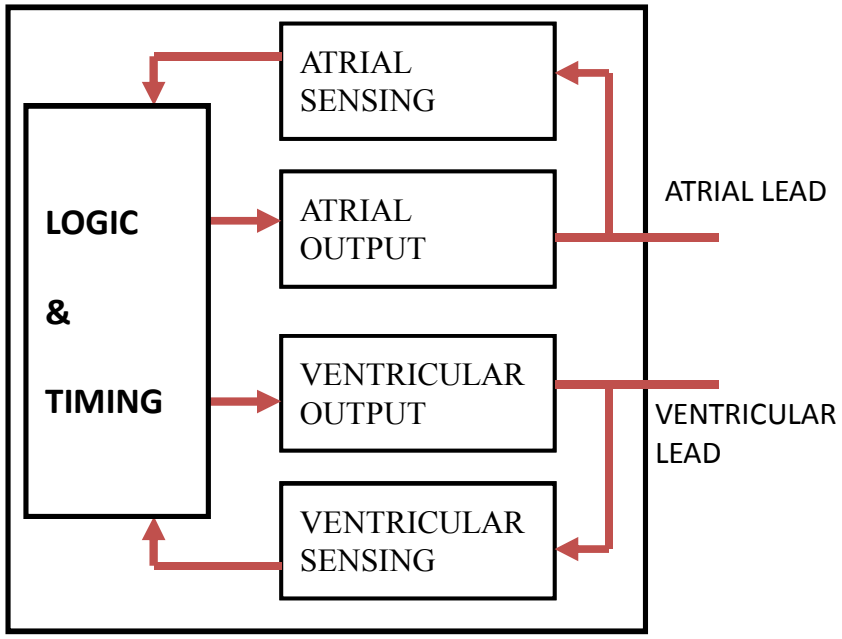




1. Physician diagnoses the symptom using pacemaker, and decides mode/parameters based on diagnostic results and knowledge/experience, specifically for a particular patient.
2. Pacemaker works (pacing and sensing) according to the configured mode and parameters.

Pulse Generator

- Signal processing hardware
- Logic and timing controller in software
  - Establishes timing cycles in response to timer events and sensed signals



Pacemaker Operating Modes

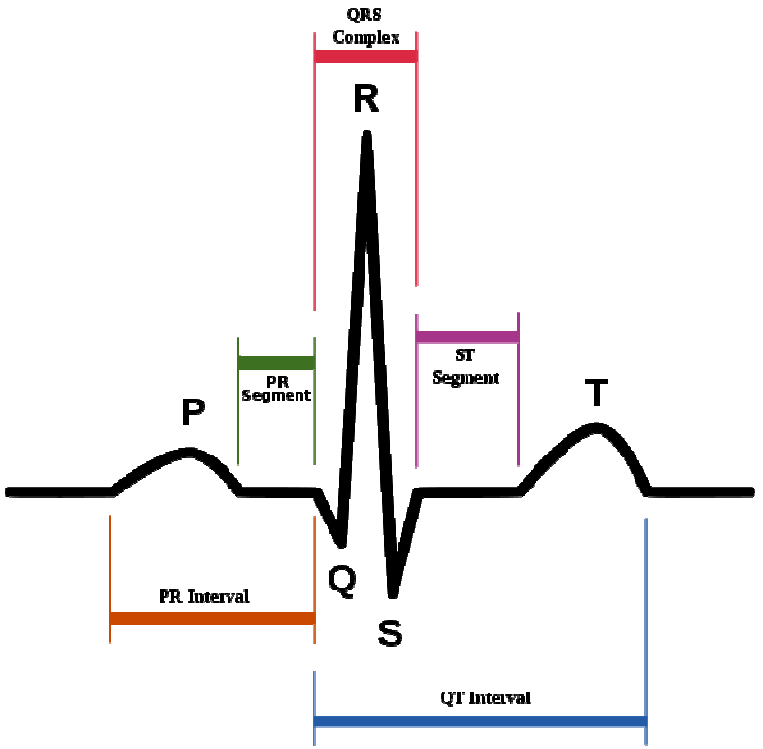
	I	II	III
Category	**Chambers Paced**	**Chambers Sensed**	**Response To Sensing**
Letters	O – None A – Atrium V – Ventricle D – Dual	O – None A – Atrium V – Ventricle D - Dual	O – None T – Triggered I – Inhibited D – Tracked

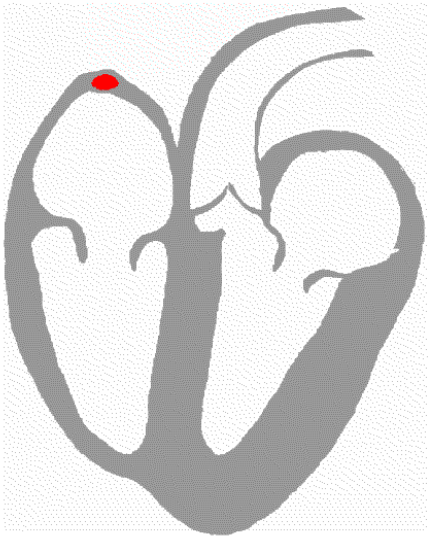
- 23 programmable pacing modes, e.g.
  - VOO: ventricle paced, no sensing (and no response to sensing)
  - VVI: ventricle paced and sensed. Ventricular sense is to inhibit the pace.
  - DDD: both chambers paced and sensed. Sense can inhibit a pace; atrial sense can trigger a ventricular pace (tracking).

Pacemaker Operating Modes

- There are 10 non-rate-adaptive *modes*, each associated with a 3-letter acronym:
  - The first refers to the chamber(s) paced by the device: V (ventricle), A (atrium), D (dual), or O (neither)
  - The second refers to the chamber(s) in which the device senses, again V, A, D, or O.
  - The third refers to the pacemaker's response to sensing: T (triggers pacing), I (inhibits pacing), D (tracked pacing), or O (neither).
    - T: During triggered pacing, a sense in a chamber shall trigger an immediate pace in that chamber.
    - I: During inhibited pacing, a sense in a chamber shall inhibit a pending pace in that chamber.
    - D: During tracked pacing, an atrial sense shall cause a tracked ventricular pace after a programmed AV delay, unless a ventricular sense was detected beforehand.

Reading ECG

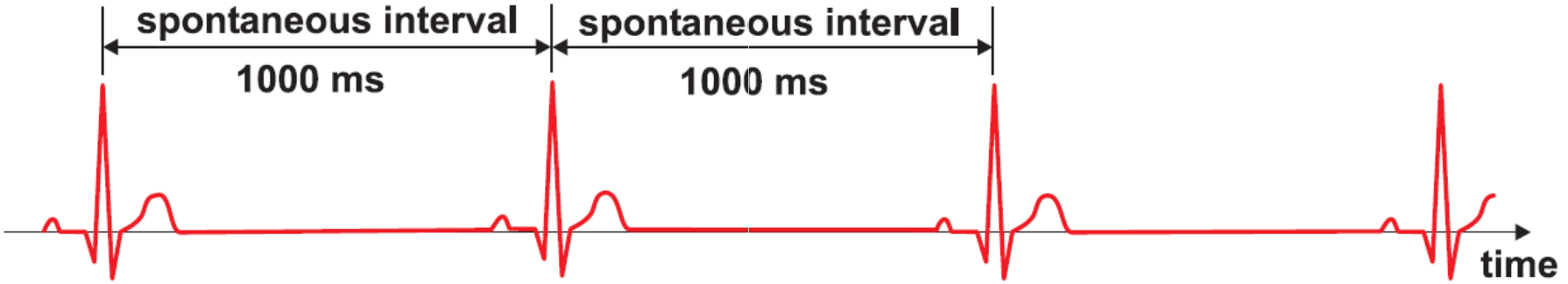




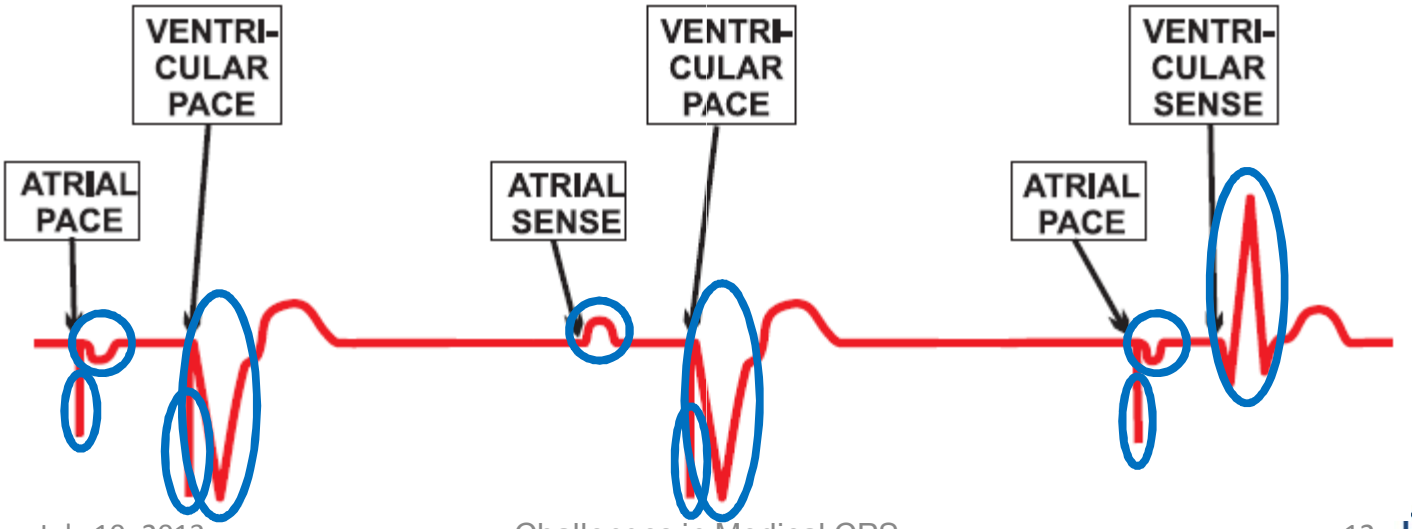
- **P wave**: normal atrial depolarization ▪ **atrial event**
- **QRS complex**
  - Depolarization of the right and left ventricles ▪ **ventricle event**
  - A recording of a single heartbeat on the ECG
- **T wave**: the repolarization (or recovery) of the ventricles.

Reading ECG

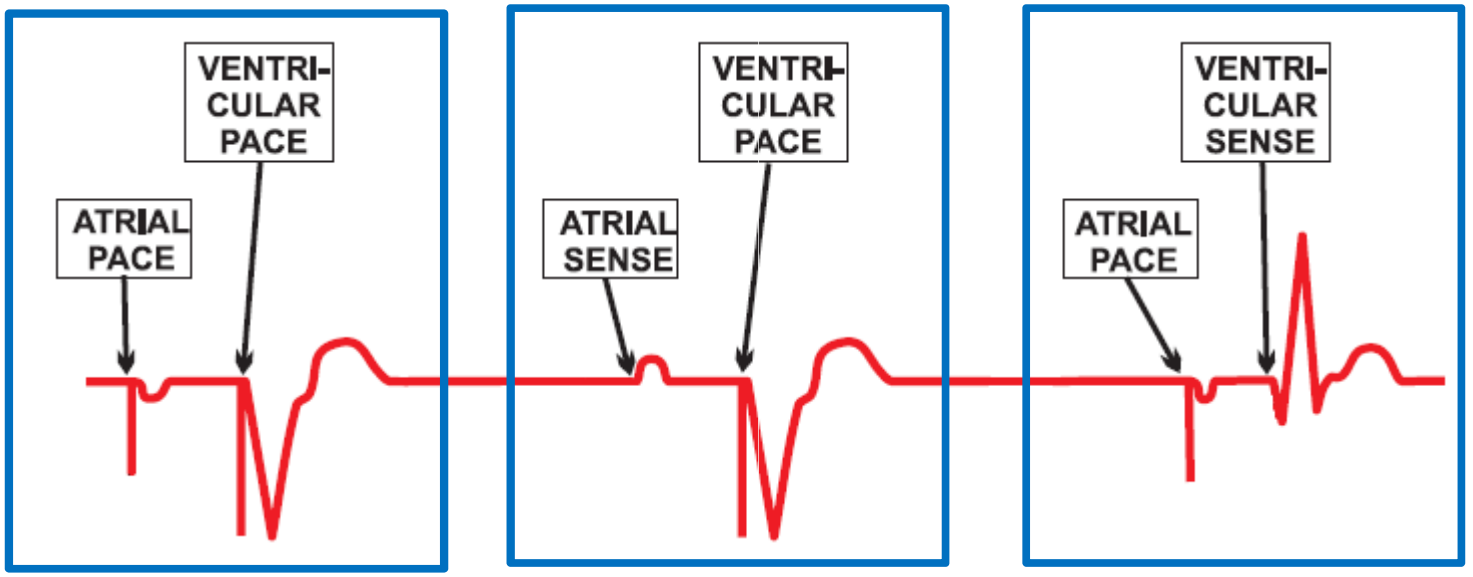
Normal Heart



Heart with problems

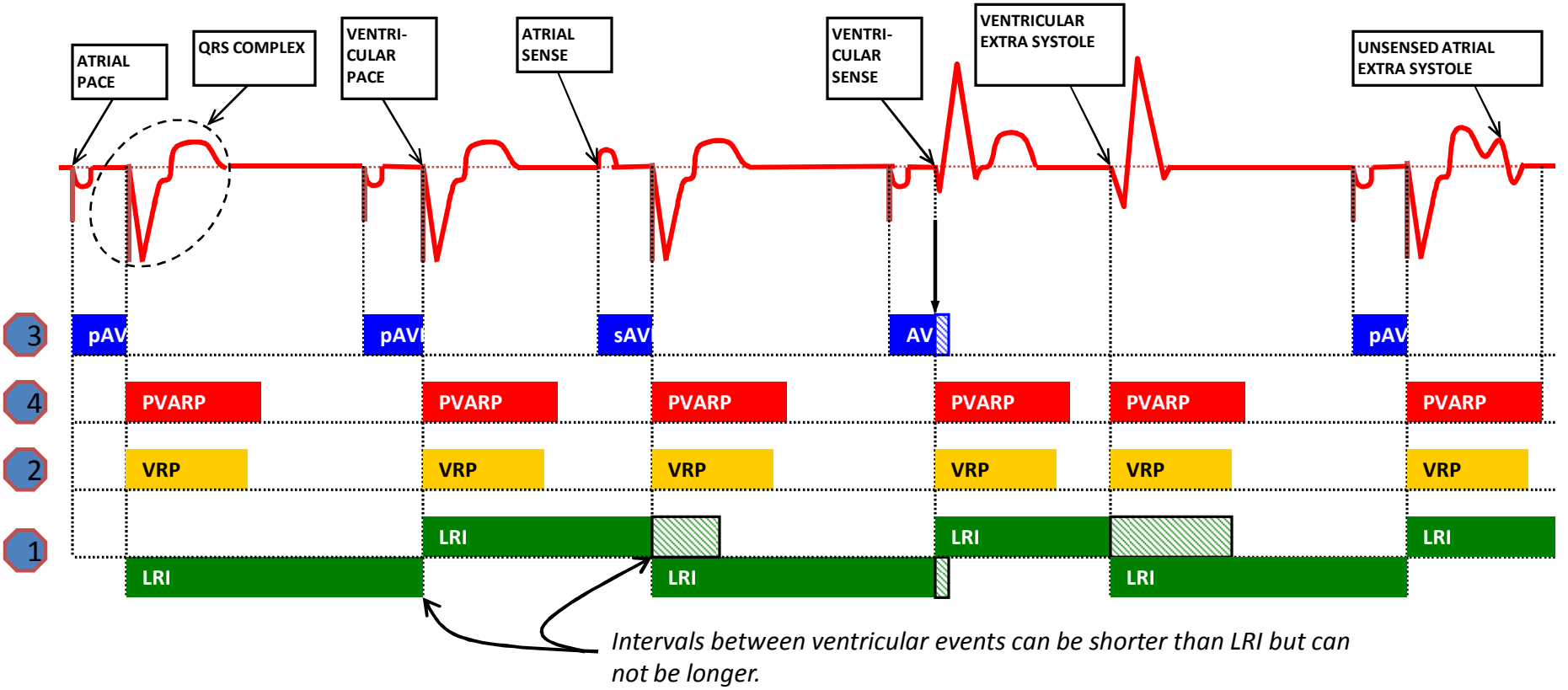


Reading ECG



- **No Sensing**: pacemaker delivers both atrial and ventricle signals
- **Atrial Sensing**
  - Atrial sensing inhibits scheduled atrial pacing
  - Pacemaker delivers ventricle pacing
- **Ventricle Sensing**: ventricle sensing inhibits scheduled ventricle pacing

Four Fundamental Timing Cycles

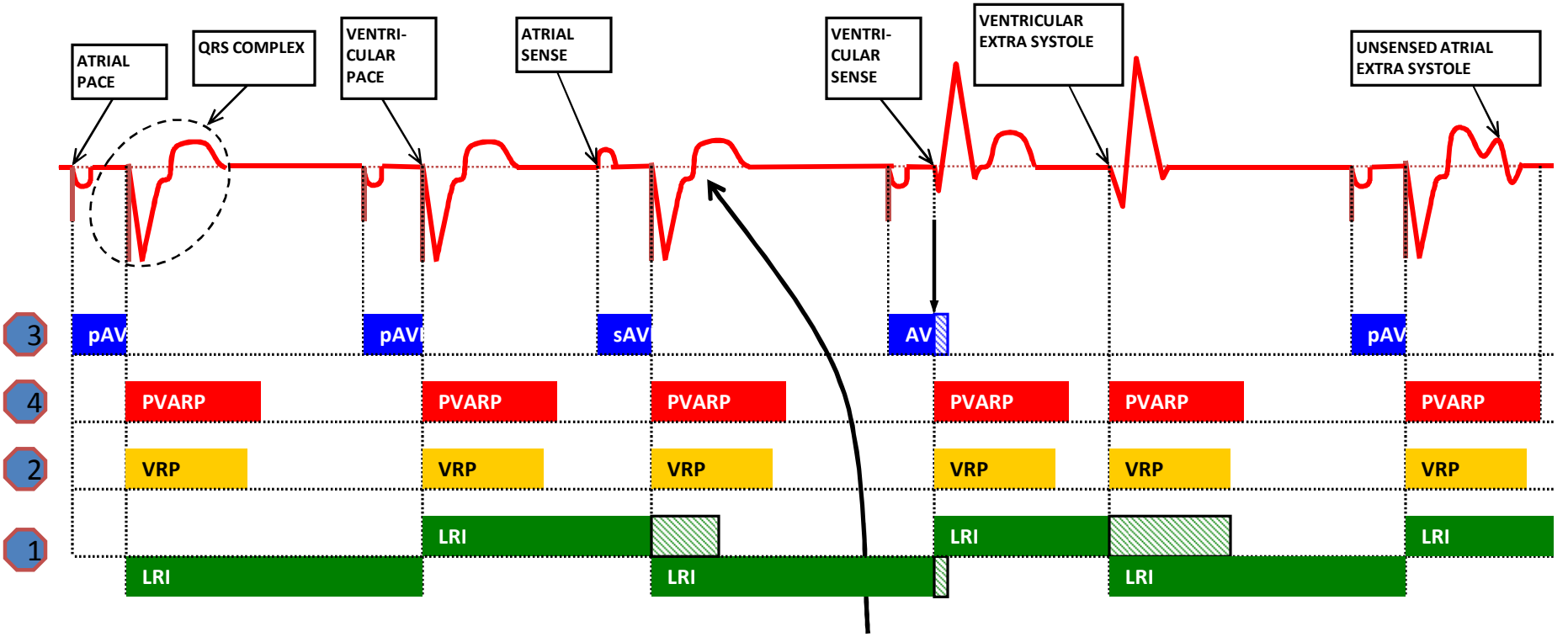


1 LRI = Lower Rate Interval

Longest interval between a paced or sensed ventricular event and the succeeding ventricular paced event with out intervening sensed events.

That is, the lowest allowable rate of ventricular events for normal operation of the heart.

Four Fundamental Timing Cycles



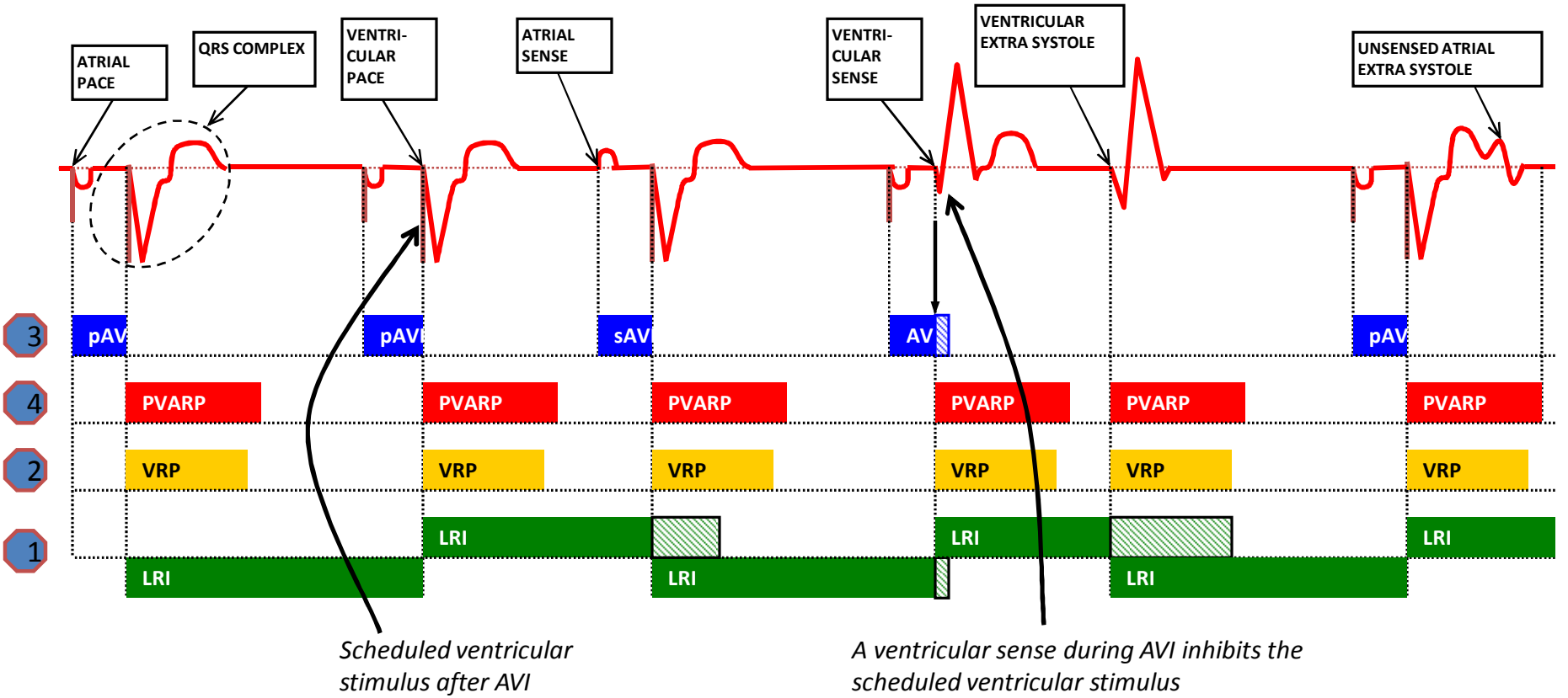
This ventricular signal is not sensed because it's in a VRP

2 VRP = Ventricular Refractory Period

Interval initiated by a ventricular event during which a new LRI cannot be initiated.

After a ventricular event, there are signals (own stimulus, QRS complex, after potential,…) which can be identified incorrectly as ventricular events, thus initiate a new LRI. VRP is used to avoid this.

Four Fundamental Timing Cycles



3 AVI = AtrioVentricular Interval

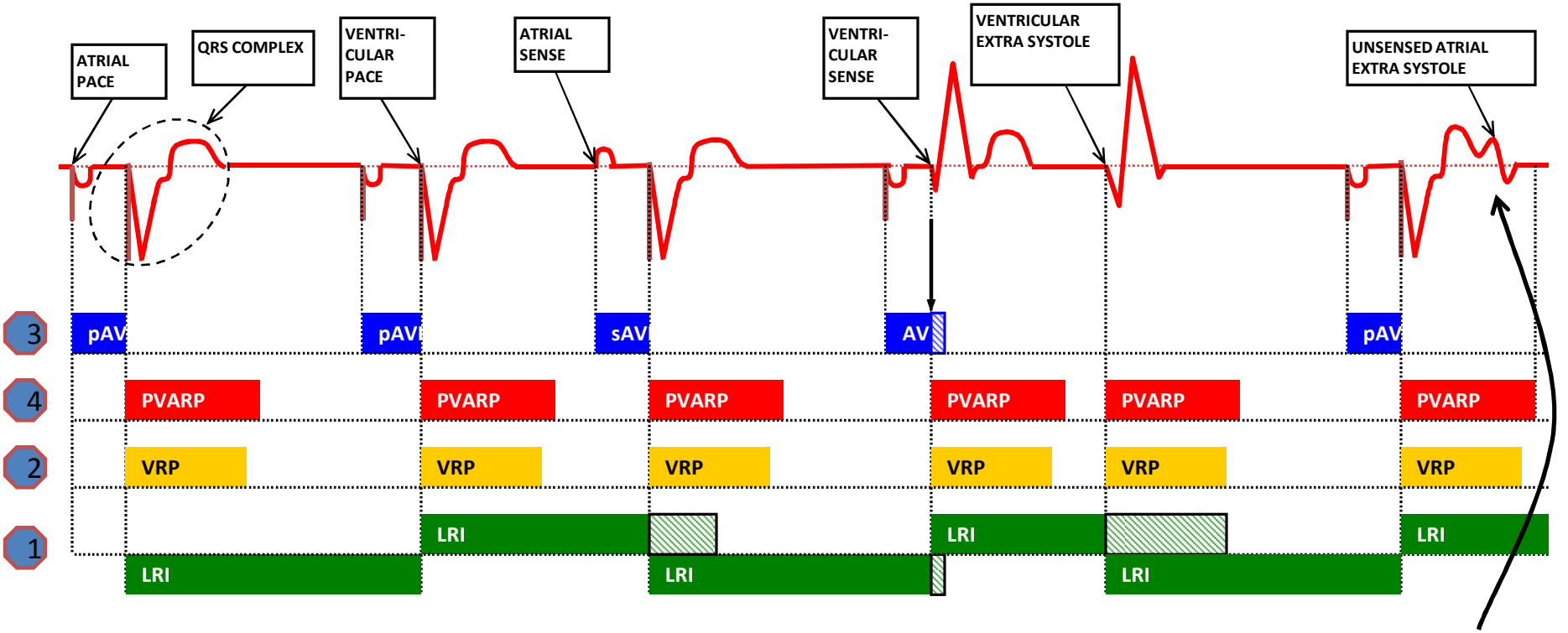
Interval between an atrial event and the scheduled delivery of a ventricular stimulus.

In a normal heart, an atrial event must always be followed by a ventricular event after some delay (AVI) ⇒ AV synchrony.

pAVI for paced atrial events; sAVI for sensed atrial events.

Maybe fixed or rate-adaptive.

Four Fundamental Timing Cycles



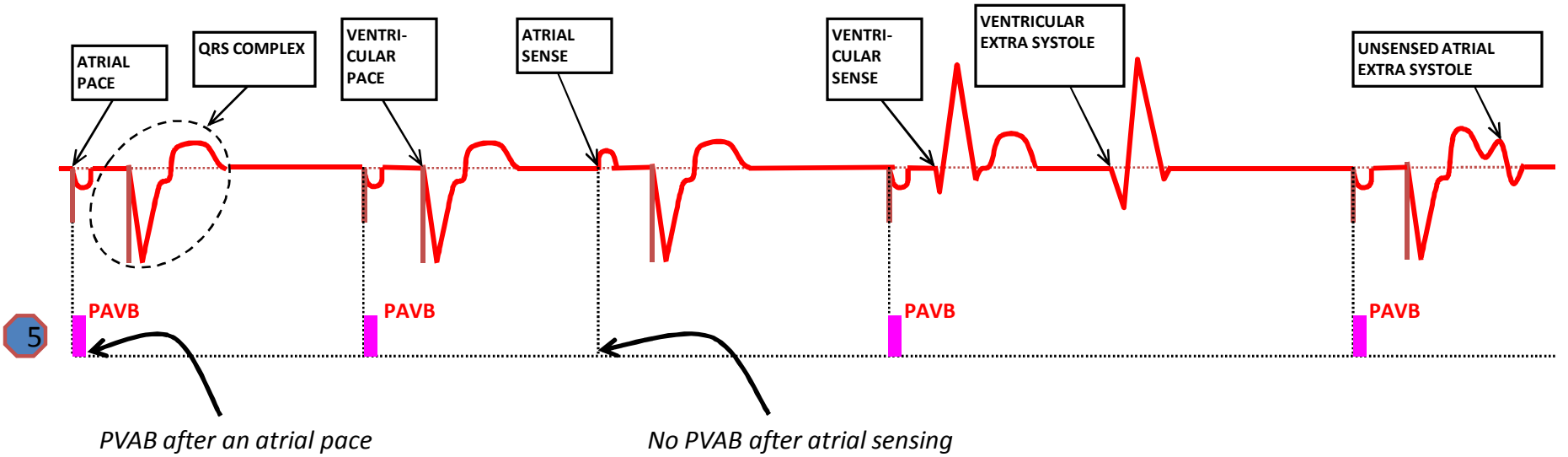
This atrial event is not sensed because it's in PVARP; no AVI is initiated

4 PVARP = PostVentricular-Atrial Refractory Period

Interval after a ventricular paced or sensed event during which an atrial event cannot initiate a new AVI.

To prevent the atrial channel from inappropriately sensing ventricular events (QRS complex, ventricular stimuli,…) or retrogradely P waves.

Fifth Timing Cycle to Prevent AV Crosstalk



AV Crosstalk

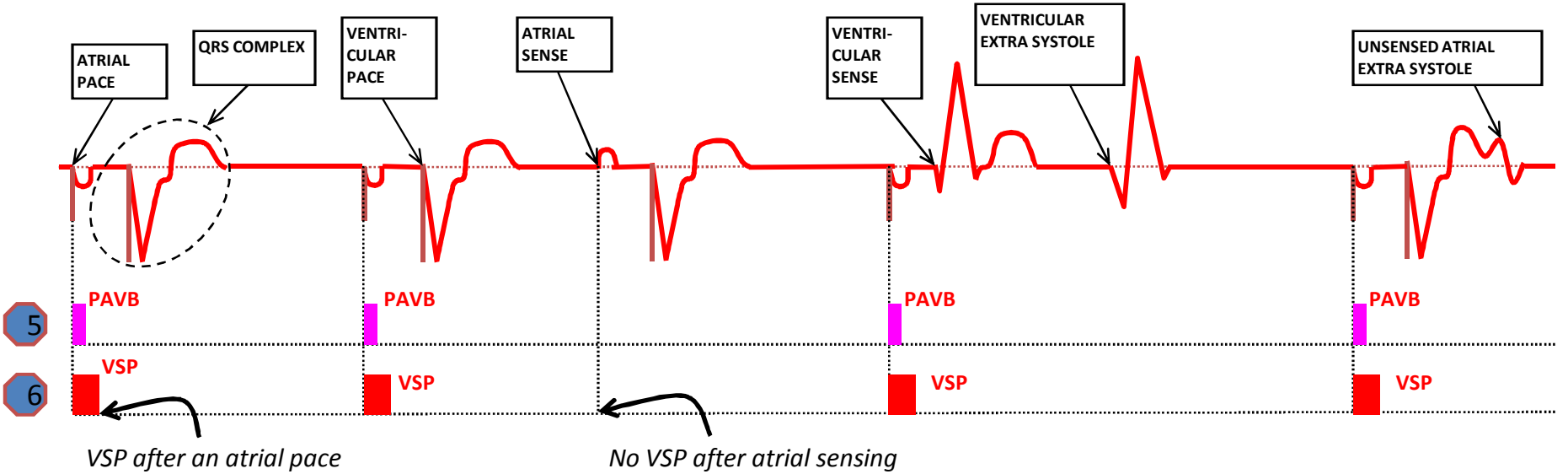
The disturbance caused by an atrial stimulus which, if sensed by the ventricular channel, may cause ventricular inhibition.

5 PAVB = Post-Atrial Ventricular Blanking

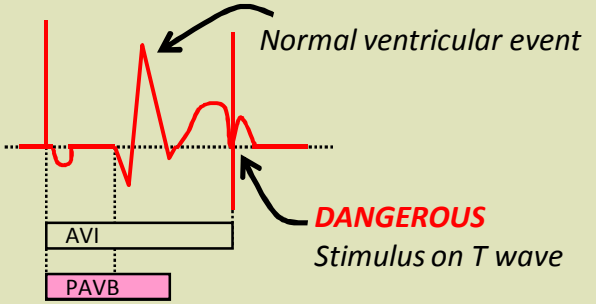
Brief interval (10-60ms) initiated by an atrial output pulse when the ventricular channel is switched off and cannot sense.

There is no PVAB after an atrial sense since it does not cause disturbance.

Sixth Timing Cycle to Prevent the Consequences of AV Crosstalk



- If PAVB is too long: normal ventricular event may not be sensed, which may cause stimulus on T wave (DANGEROUS for the heart).
- If PAVB is too short: crosstalk may still happen.



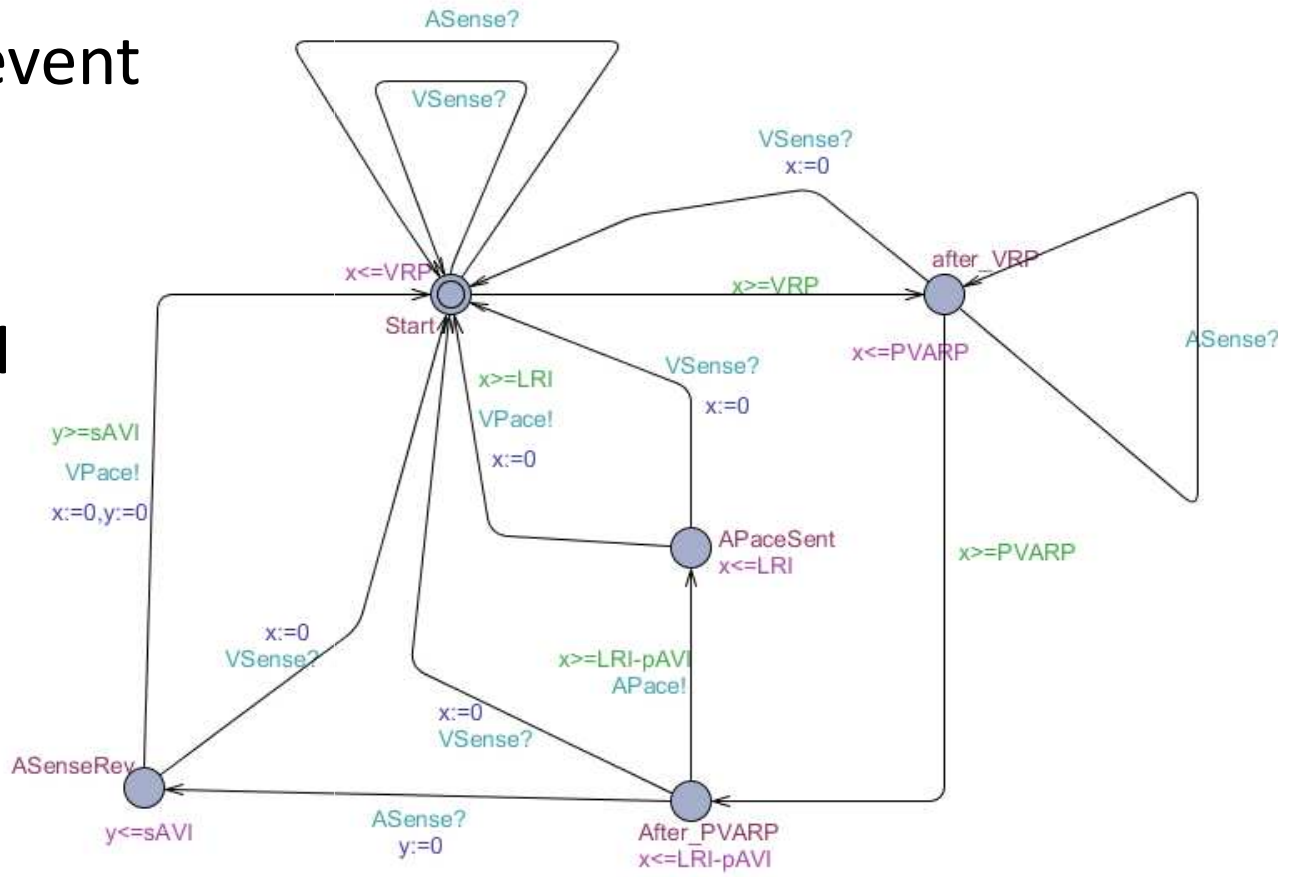
6 VSP = Ventricular Safety Pacing

First part of AVI (PAVB < VSP < AVI) during which ventricular channel can sense; a signal sensed in VSP but not in PAVB will trigger a premature ventricular stimulus at the end of VSP (thus shorten the current AVI).

VSP does not prevent crosstalk, just prevents its consequences.

UPPAAL Model

- LRI, VRP, PVARP start at a ventricular event
  - Measured by x
- AVI starts in the middle of LRI
  - Measured by y



Pacemaker Summary

- Simple device with very tight constraints
  - Energy constraints
  - Timing constraints
- Advanced modes require more complex logic
  - E.g., adjust for physical activity
- Security concerns
  - Remote programming is a new risk
- Pacemaker challenge – case study for high-assurance development

Outline

- Trends in Medical CPS
- Stand-alone devices
  - Pacemaker
  - Infusion Pump
- Medical device interoperability
  - Promises and challenges
  - IEEE/ISO 11073 standard
  - Clinical scenarios as virtual devices
  - Physiological Closed-loop Systems

Infusion Pumps

- Infusion pumps are medical devices that deliver fluids, (nutrients and medications) into a patient's body in a controlled manner
- Infusion pumps are used worldwide in patient care, as well as in the home

Infusion Pump Safety

- From 2005 through 2009, FDA received approximately 56,000 reports of adverse events associated with the use of infusion pumps, including serious injuries and deaths [1].
  - During this period, 87 infusion pump recalls were conducted by firms to address identified safety problems.
- The most common types of problems
  - **Software Defects**
  - User Interface Issues
  - Mechanical or Electrical Failures

[1] U.S. Food and Drug Administration, Center for Devices and Radiological Health. White Paper: Infusion Pump Improvement Initiative, April 2010.

Patient-Controlled Analgesia (PCA)

- Purpose
  - Pain-relief treatment (opioids, e.g., morphine)
- Operation parameters
  - VTBI (Volume To Be Infused)
  - Basal rate
  - Bolus dose
    - additional amount of drug can be requested by the patient

Bolus-Request button

PCA Hazards

- Overinfusion
  - Opioids can cause respiratory distress
    - the patient can stop breathing
- Air in line
  - Air bubbles entering blood stream with medication
- Underinfusion
  - Can limit effectiveness of pain management

Causes of Overinfusion

- Incorrect dose
  - Varying sensitivity: hard to predict the right dose
    - Many hospitals disable basal infusion
- Excessive bolus
  - "PCA by proxy" makes the problem worse
- Free flow of medication

- Many of these causes cannot be mitigated by the device itself!

Hazards -> Safety Requirements

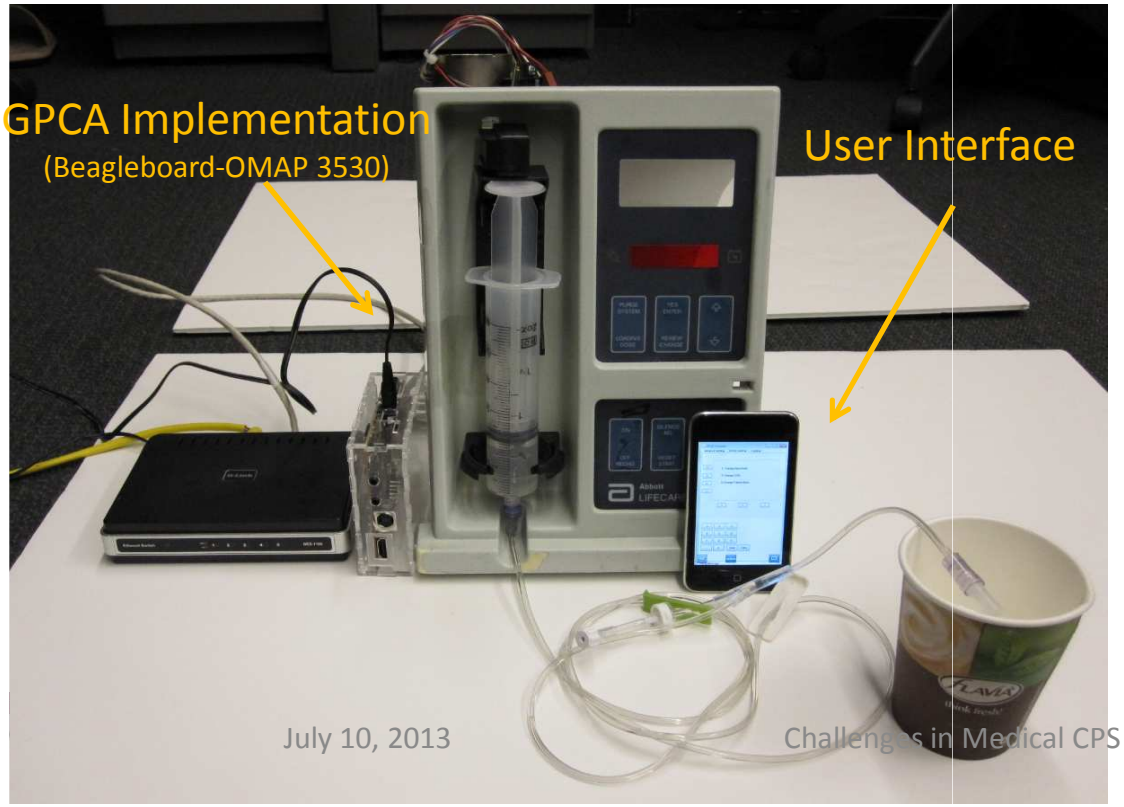
- Prescribed dose cannot be exceeded
- Prescribed rate is closely adhered to
- When an alarm is raised, the pump should be stopped quickly enough
- Minimum interval between boluses should be enforced

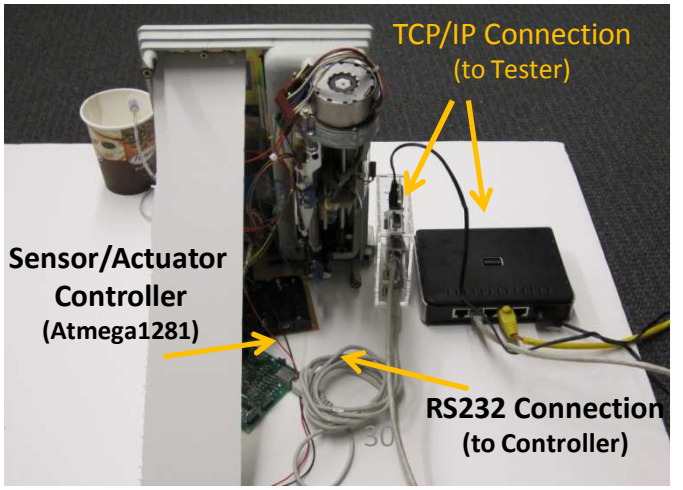
High Assurance Development

- Use formal methods for modeling, verification, and code generation
- GPCA (Generic PCA) project
  - Develop a set of artifacts
    - Design documents, models, verification results, code, etc.
  - Community resource to apply and compare various development methods
  - Inform FDA on modern development practices

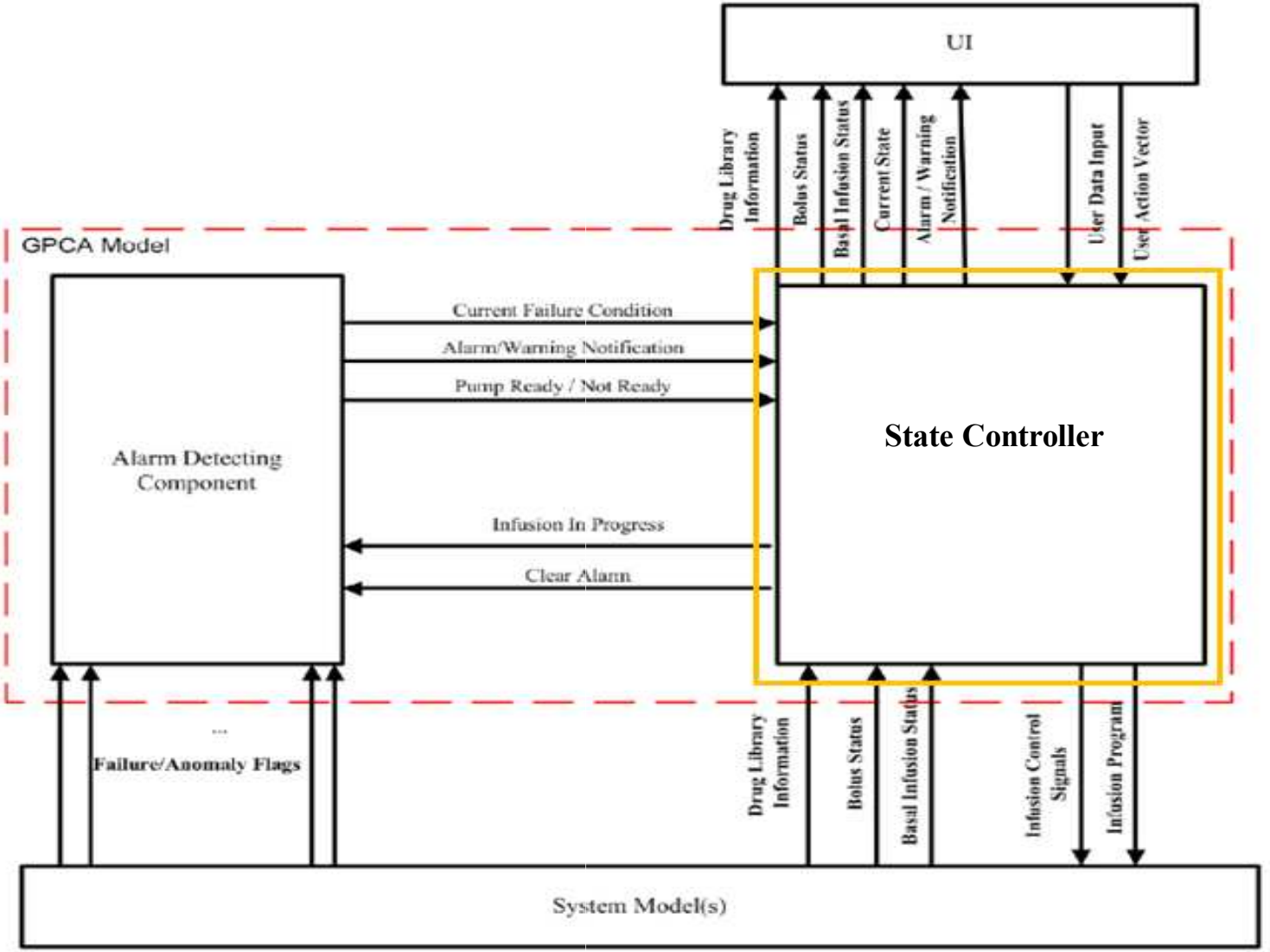
GPCA Project

- Open platform for medical device research
- Support a variety of pump hardware

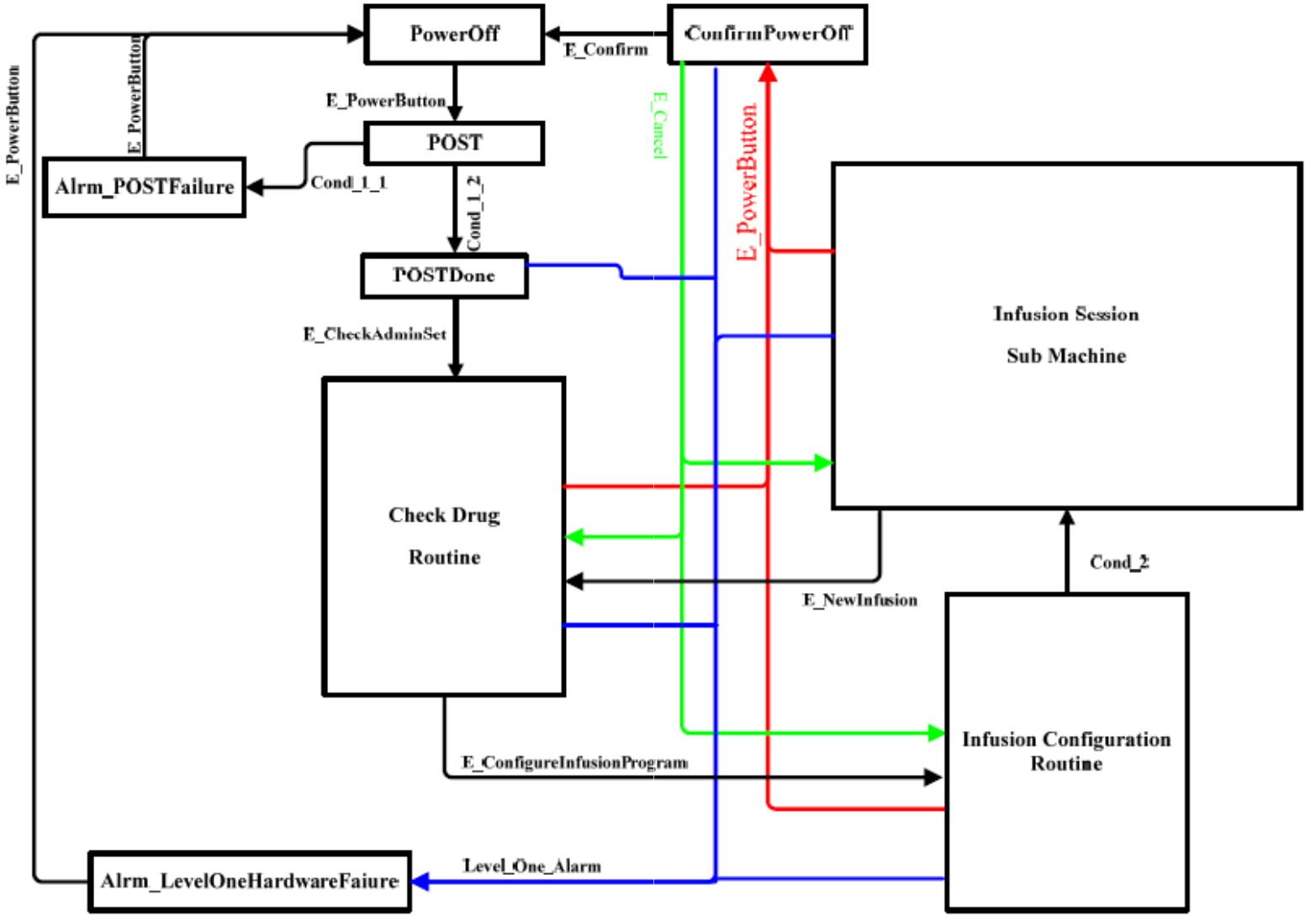




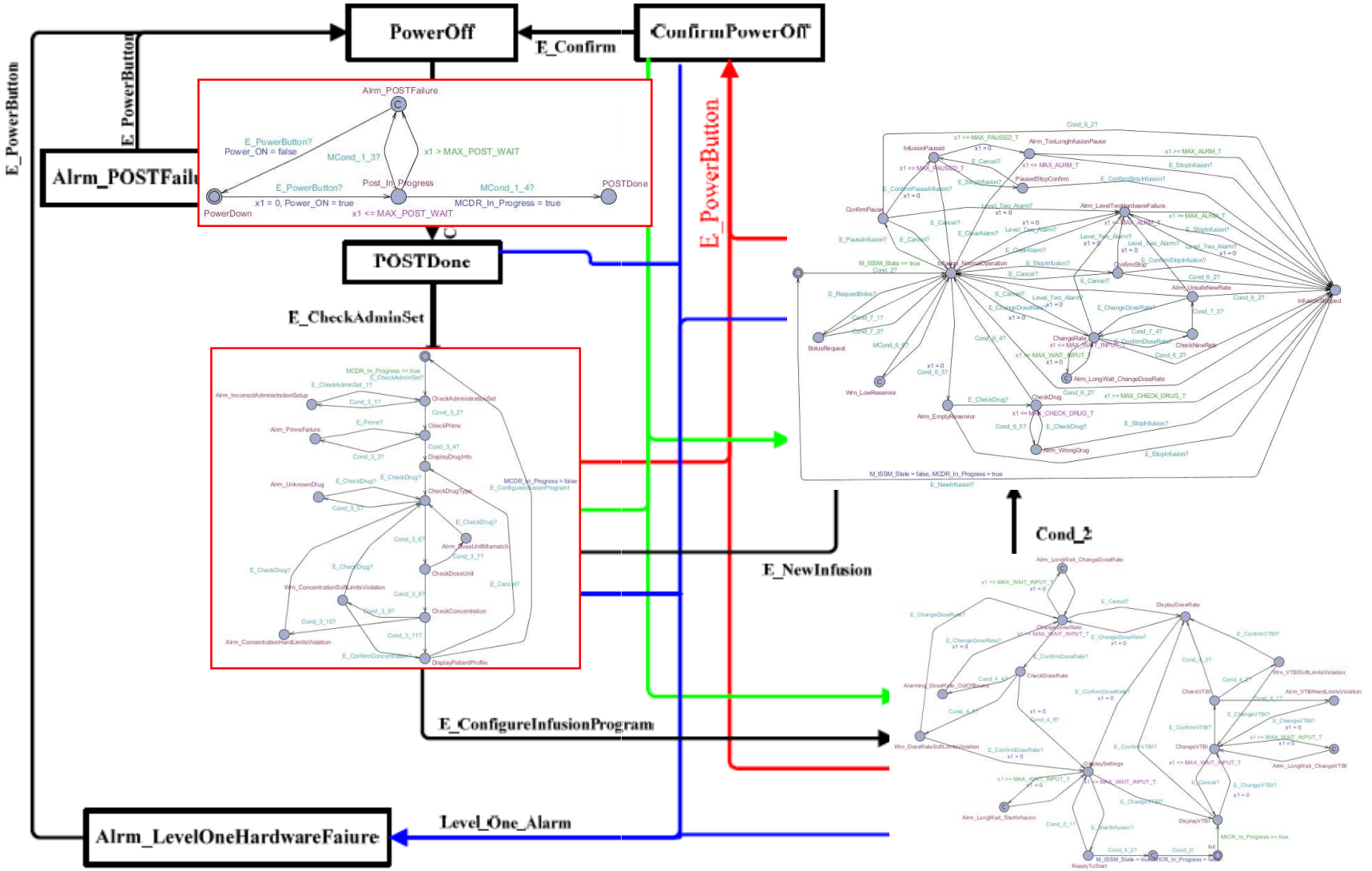
GPCA Architecture



GPCA State Controller



Timed Automata Modeling



Code Generation

- Platform-independent code is generated using TIMES tool
- Platform-dependent glue code is added manually, and separately for each platform
  - There is a lot of glue code
  - Declarations of platform APIs and API calls
- Goal of the follow-up projects:
  - Reduce the amount of glue code

Infusion pump summary

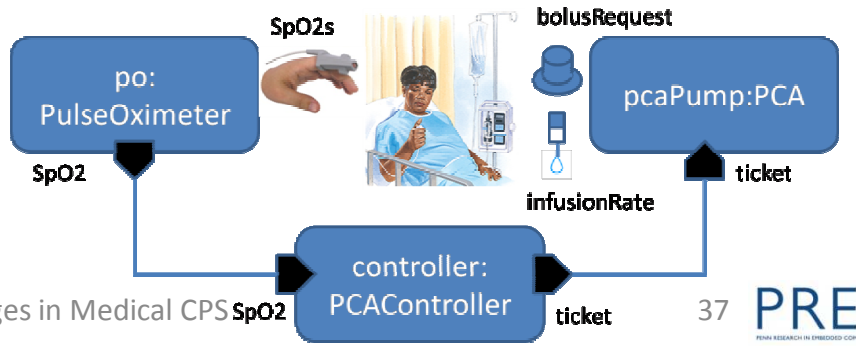
- A PCA pump is a very simple device
- Main lesson to learn:
  - Even a simple device can lead to safety problems
- Culprits:
  - Market pressures relax safety culture
  - Safety assessment technology needs improvement

Outline

- Trends in Medical CPS
- Stand-alone devices
  - Pacemaker
  - Infusion Pump
- Medical device interoperability
  - Promises and challenges
  - IEEE/ISO 11073 standard
  - Clinical scenarios as virtual devices
  - Physiological Closed-loop Systems

Connectivity and Interoperability

- Clinical scenarios involve multiple devices
- From stand-alone devices…
  - Each device with its own displa
- … to integrated displays …
  - MDDS: limited functionality
- … to enhanced functionality via interoperation



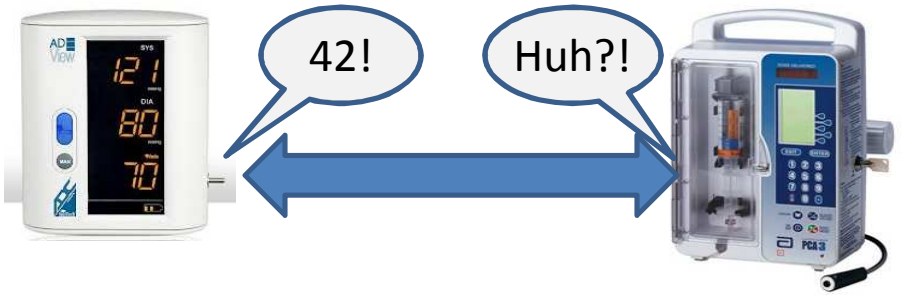
Why Interoperability?

- What is so special about medical devices?
  - We never talk about automotive interoperability…
- Other safety-critical domains rely on highly integrated systems
  - Integrators ensure that all parts in a car or plane are compatible

- Patients are treated by a collection of devices from different vendors
  - Who is the integrator?

Interoperability Challenges

- Interoperability is more than connectivity
  - Devices need to understand each other
  - Need ontologies and ontology-aware protocols



- Safety assessment requires a new approach

ISO/IEEE 11073

- Medical device interoperability standard
  - Domain information model
  - Service model
  - Communication model
- Two variants:
  - Point-of-care devices (POC)
    - Much more complex
  - Personal health devices (PHD)

Architecture

- Manager-mediated communication

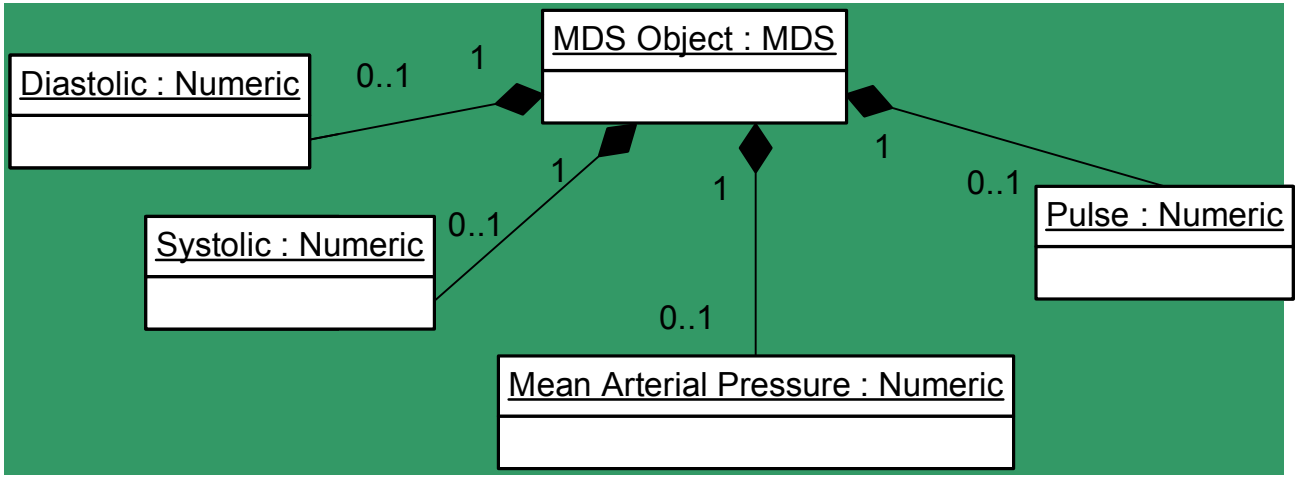
- Agents (devices)
  - Limited capabilities
  - Fixed configurations
  - Intermittent connections to one manager at a time
- Manager hosts application logic

Domain Information Model

- Collection of classes describing the domain
  - Medical Device System (MDS)
  - Metric – models different forms of measurements
  - Persistent Metric Store (PM) – provides mechanism to store data for a period of time
  - Scanner – groups and optimizes data transmission
- Classes contain attributes and access methods
  - ASN.1 is used to define attribute types
  - Abstract definition can be supported in multiple languages

MDS class

- Defines attributes of a device model
  - Device type
  - Configuration used
  - Message formats
  - Time handling
  - Battery status
- Attributes can be queried by the manager
- Example:
  - Blood pressure monitor



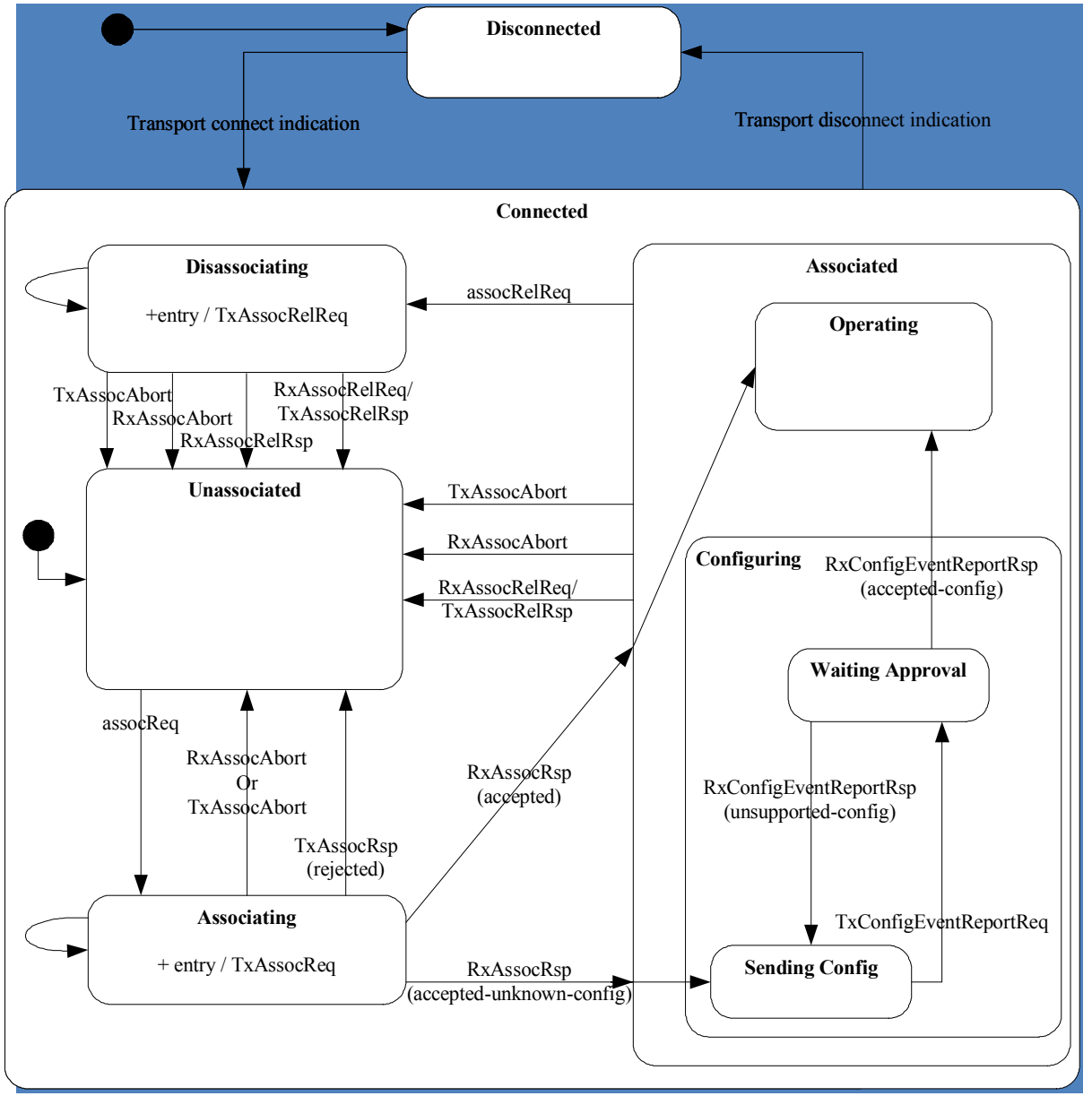
Service Model

- Event Reporting Service
  - Configuration report
    - Well-known configurations can be names, others need to be described
  - Data Update
- Object Access Service
  - Get/Set access to DIM attributes
- Association Service
  - Establish connection between agent and manager
- Format described in ASN.1

Communication Model

- Communication characteristics
  - Point to point
  - Reliable or “best effort”
- Connection state machine
- Legal interactions in each state
- Supported transport protocols:
  - USB, Bluetooth, etc.
- Conversion Service

Connection State Machine



- Connected does not mean associated!
- Agent initiates association
- Manager accepts well-known configurations, o/w requests configuration report
- All data reporting is in the Operating state

Concerns about 11073

- Extremely complex
  - Aims at a comprehensive solution at all levels
  - Many optional parts give rise to dialects
- Few available implementations
  - Mostly proprietary
  - Interoperability within one brand of devices
- Many device classes are standardized
  - What about new devices?
- Not a bad standard, but a complex problem!

Safety Challenges

- How to we argue that an MCPS assembled at bedside is safe?
  - It is not sufficient to have individually safe devices
  - Interactions need to be safe as well
- Demonstrate that a unexpected behavior or failure of a device does not affect safety of connected devices
- Need an assurance approach that would be effective with regulatory agencies

Certification Challenges

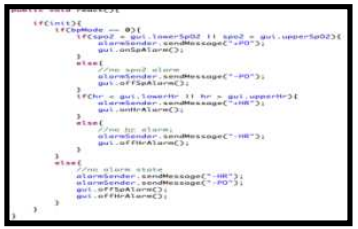
- Safety-critical systems are subject to regulatory approval
  - In the US, FDA evaluates devices for safety and effectiveness before they can go on the market
- Each device or system is approved for specific purposes
- Every collection of interconnected devices is a new device that needs approval
  - Unsustainable because of the number of combinations

Sell Me a Safety Interlock…

- Hospitals have a variety of devices, often from various manufacturers,
  - A limited variety of multi-device clinical scenarios
- Hospitals need software applications that would allow interoperating devices
  - They do not develop these applications in house
- Yet, it is impossible to buy such a software application
  - Only complete systems are approved!

Virtual Medical Devices

- Interoperability enables the concept of Virtual Medical Devices
  - A set of medical devices coordinating over a network for a specific clinical scenario

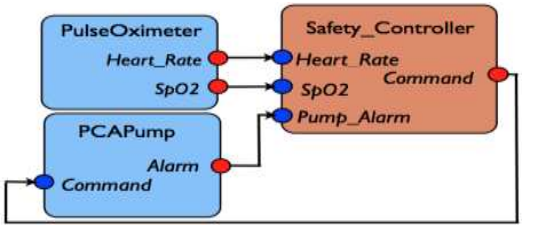


Device Coordination Logic

+

Medical Device Types

=

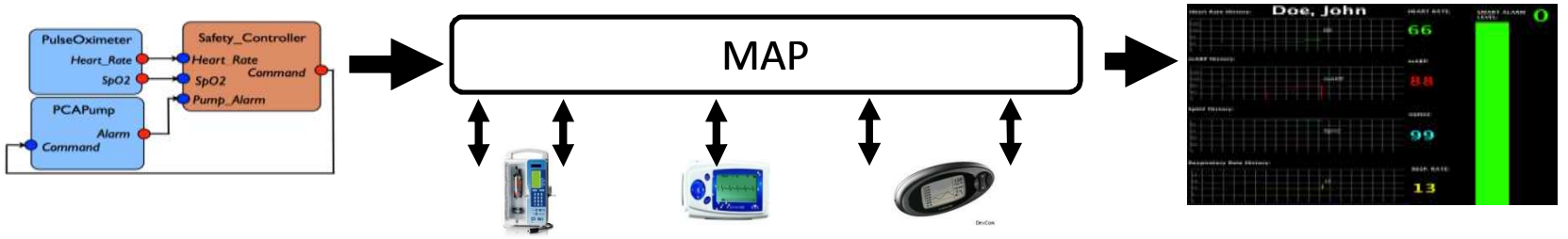


Virtual Medical Device (VMD)

- VMD does not physically exist until instantiated at a hospital

Medical Application Platform

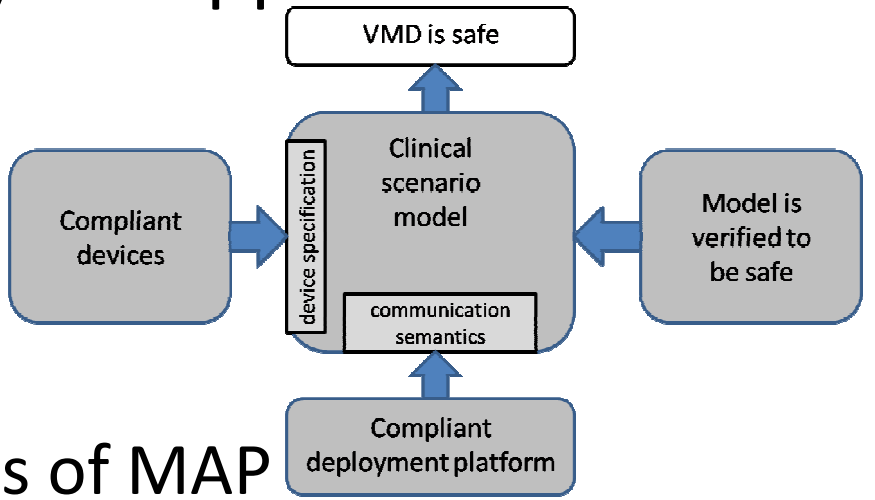
- Ensures that a VMD is instantiated correctly



- VMD instatiation:
  - Clinician selects a VMD
  - Clinical engineer supplies appropriate devices
  - MAP binds devices into a VMD instance
- Research prototype
  - MDCF/MIDAS

Assurance Approach

- Clinical scenarios (VMDs) are approved for safety w.r.t.
  - Device models that capture assumptions on device behavior
  - Communication semantics of MAP



- MAP is approved for safety w.r.t.
  - Communication protocol assures that only compliant devices can be associated
  - Communication semantics between devices

Interoperability summary

- IEEE/ISO 11073 lays the groundwork for interoperable medical systems
  - Need community effort and open-source reference implementations to make it useful
- Does VMD-based approach offer a suitable regulatory pathway?
  - Remains to be seen

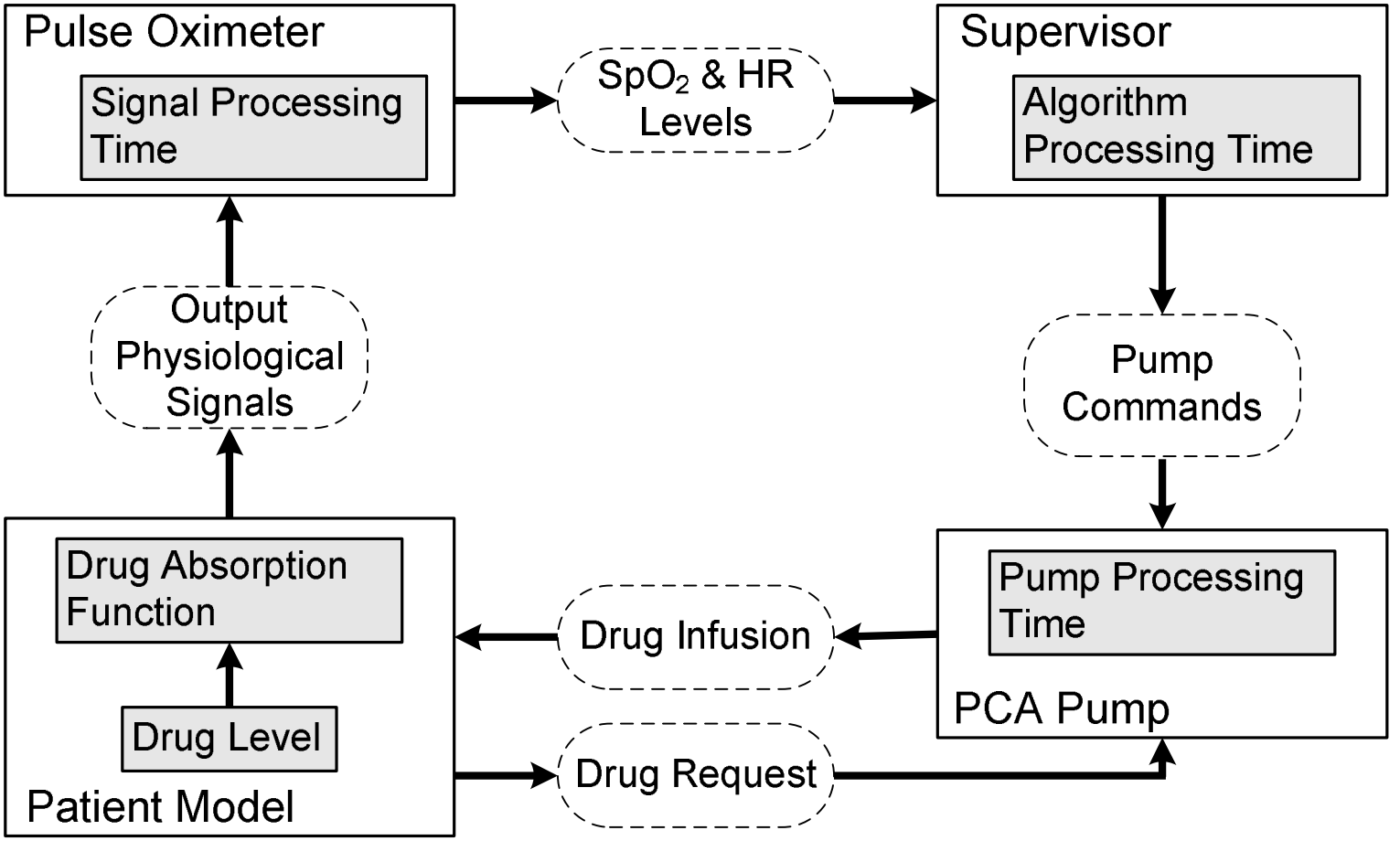
Outline

- Trends in Medical CPS
- Stand-alone devices
  - Pacemaker
  - Infusion Pump
- Medical device interoperability
  - Promises and challenges
  - IEEE/ISO 11073 standard
  - Clinical scenarios as virtual devices
  - Physiological Closed-loop Systems

Case Study: PCA Safety Interlock

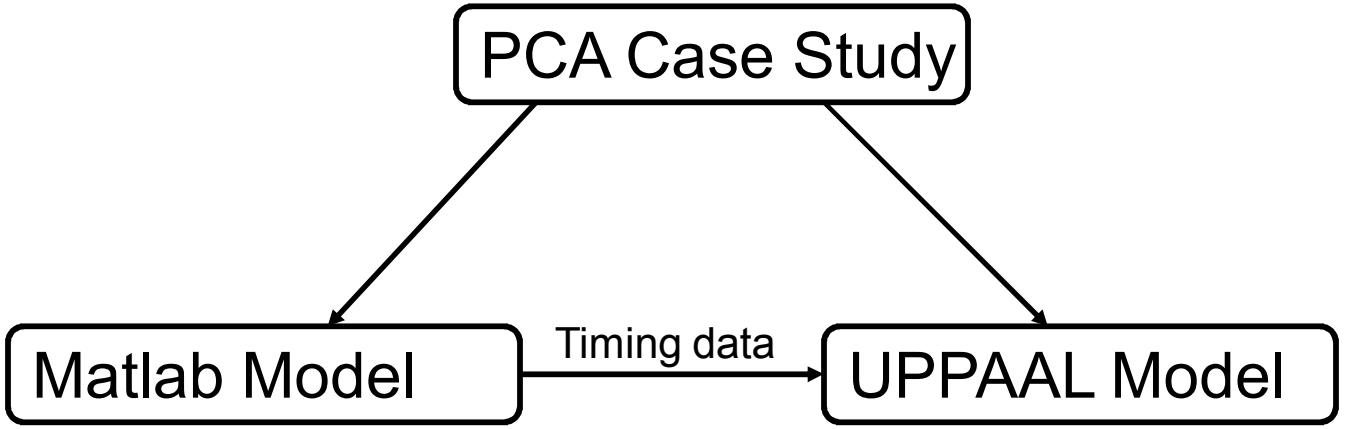
- Physiological closed loop:
  - Pump operation is controlled by vital signs
- Stop the pump if signs of respiratory distress are detected
- Enhanced patient safety
  - Continuous monitoring
  - Potential for personalized settings
- Can reduce treatment effectiveness
  - Thresholds may be set too conservatively

Control Loop



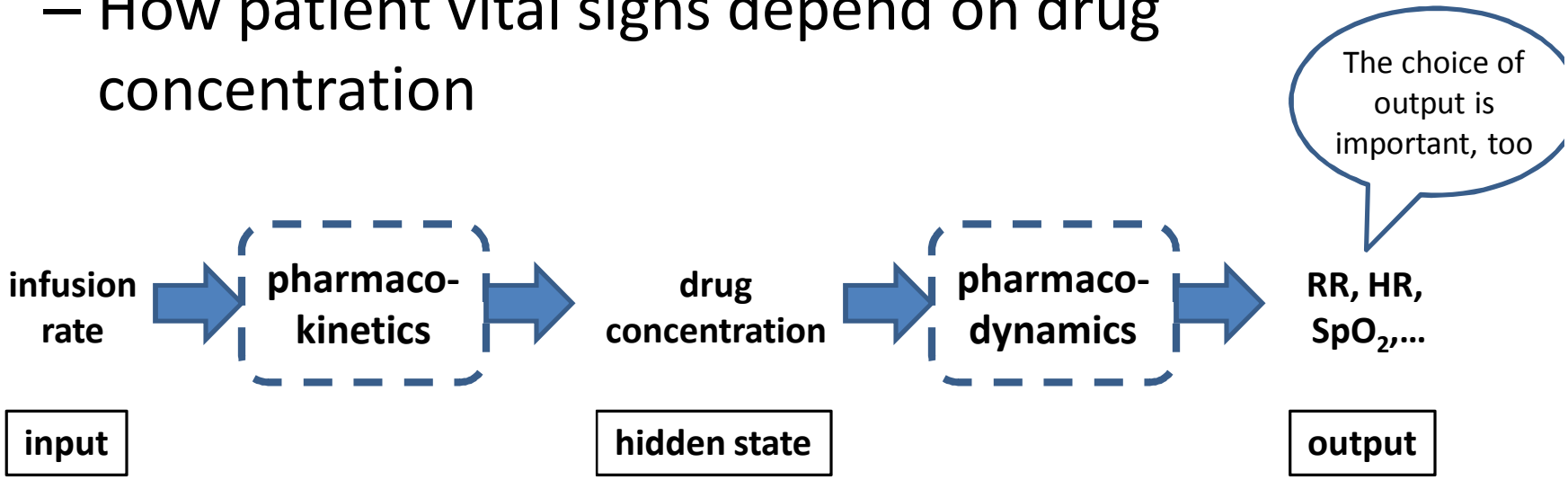
Modeling approach

- Matlab/Simulink captures detailed dynamics
- Simulation provides timing data to tune the more abstract UPPAAL model
- Formal verification in UPPAAL



Patient Modeling

- Pharmacokinetics:
  - How infusion rate affects drug concentration in the bloodstream
- Pharmacodynamics:
  - How patient vital signs depend on drug concentration



Patient Model

- Derived from pharmacokinetics model for intravenous delivery of anesthetic drugs

$$\begin{bmatrix}\dot{C}_1\\ \dot{C}_2\\ \dot{C}_3\end{bmatrix} = \underbrace{\begin{bmatrix}-(k_{12}+k_{13}+k_{10}) & k_{21} & k_{31}\\ k_{12} & -k_{12} & 0\\ k_{13} & 0 & -k_{31}\end{bmatrix}}_{\mathbf{A}} \begin{bmatrix}C_1\\ C_2\\ C_3\end{bmatrix} + \underbrace{\begin{bmatrix}\frac{1}{V_1}\\ 0\\ 0\end{bmatrix}}_{\mathbf{B}} I$$

$$dl = \underbrace{\begin{bmatrix}1 & 0 & 0\end{bmatrix}}_{\mathbf{C}} \begin{bmatrix}C_1\\ C_2\\ C_3\end{bmatrix}$$

Modeling Patient specific behavior – model with uncertain parameters

$$k_{ij} \in \left[\hat{k}_{ij} - \Delta k_{ij}, \hat{k}_{ij} + \Delta k_{ij}\right]$$

$$V_1 \in \left[\hat{V}_1 - \Delta V, \hat{V}_1 + \Delta V\right]$$

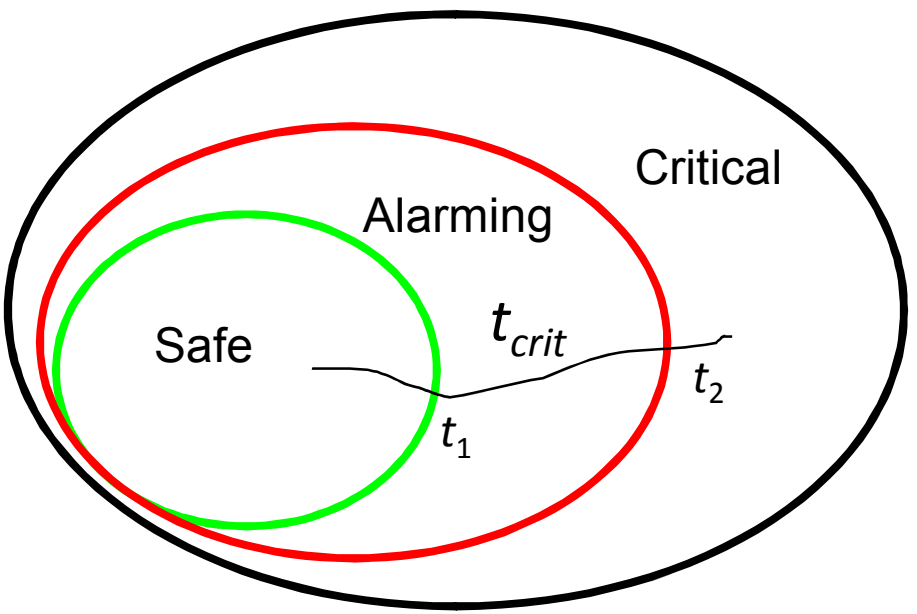
- Pharmacodynamics is much more complex
  - Not modeled in this case study

Patient Model Outputs

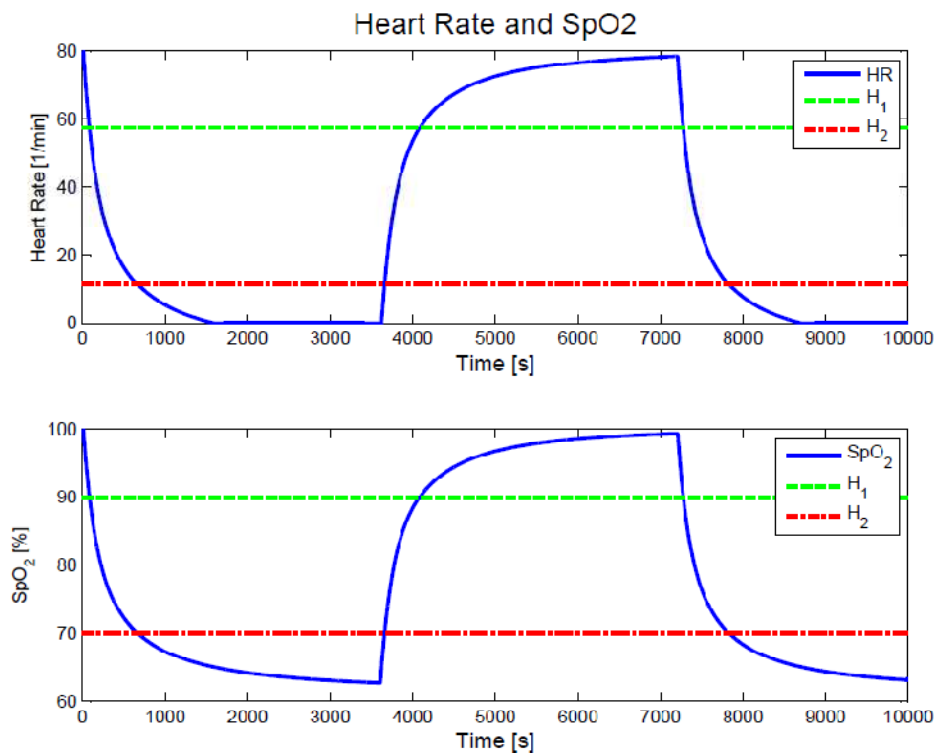
SpO_2 level and heart rate

$$c_{min} + a_1 e^{-\lambda_1 t} + a_2 e^{-\lambda_2 t} + a_3 e^{-\lambda_e t}$$

Patient Critical Regions

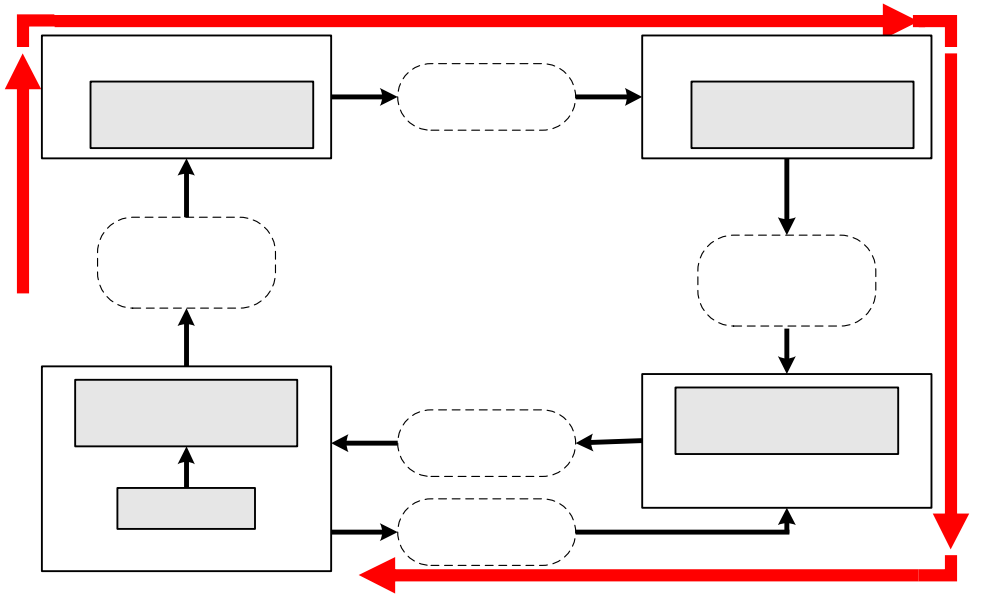


Patient Response to Drug



Key Safety Property

Pump stops in time if total delay <= t_{crit}



Total delay is the sum of:

- tPOdel: worst case delay from PO (1s)
- tnet: worst case delay from network (0.5s)
- tSup: worst case delay from Supervisor (0.2s)
- tPump: worst case delay from pump (0.1s)
- tP2PO: worst case latency for pump to stop (2s)
- tcrit: shortest time the patient can spend in the alarming region before going critical

Obtaining t_{crit}

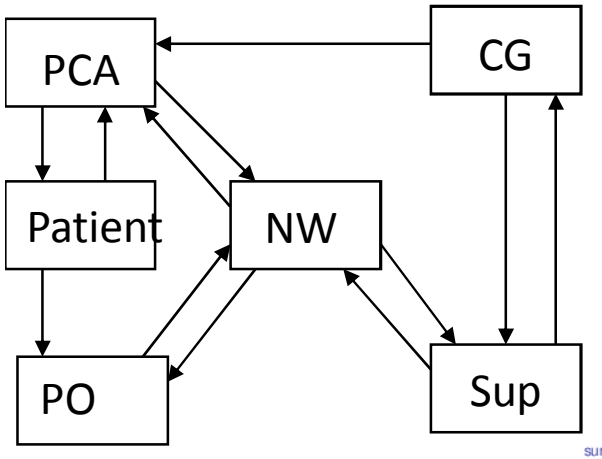
- For the patient model with fixed parameters t_{crit} determined analytically
- For model with uncertain parameters
  - Matrices **A**, **B**, **C** belong to specified regions
  - Providing a bound on t_{crit}

$$\tilde{t}_{crit} = \frac{1}{||\tilde{\mathbf{A}}||} \ln \left(\frac{\frac{|\Delta H|}{gain}}{||\tilde{\mathbf{C}}|| \cdot \left(||\tilde{x}_0|| + \frac{||\tilde{\mathbf{B}} u_i||}{||\mathbf{A}_{max}||} \right)} + 1 \right)$$

$$\tilde{\mathbf{A}} = \underset{\mathbf{A} \in \Re\{\mathbf{A}\}}{\operatorname{argmax}} ||\mathbf{A}||, \tilde{\mathbf{B}} = \underset{\mathbf{B} \in \Re\{\mathbf{B}\}}{\operatorname{argmax}} ||\mathbf{B}\mathbf{u_i}||, \tilde{\mathbf{C}} = \underset{\mathbf{C} \in \Re\{\mathbf{C}\}}{\operatorname{argmax}} ||\mathbf{C}||$$

$$\mathbf{A}_{min} = \underset{\mathbf{A} \in \Re\{\mathbf{A}\}}{\operatorname{argmin}} ||\mathbf{A}||$$

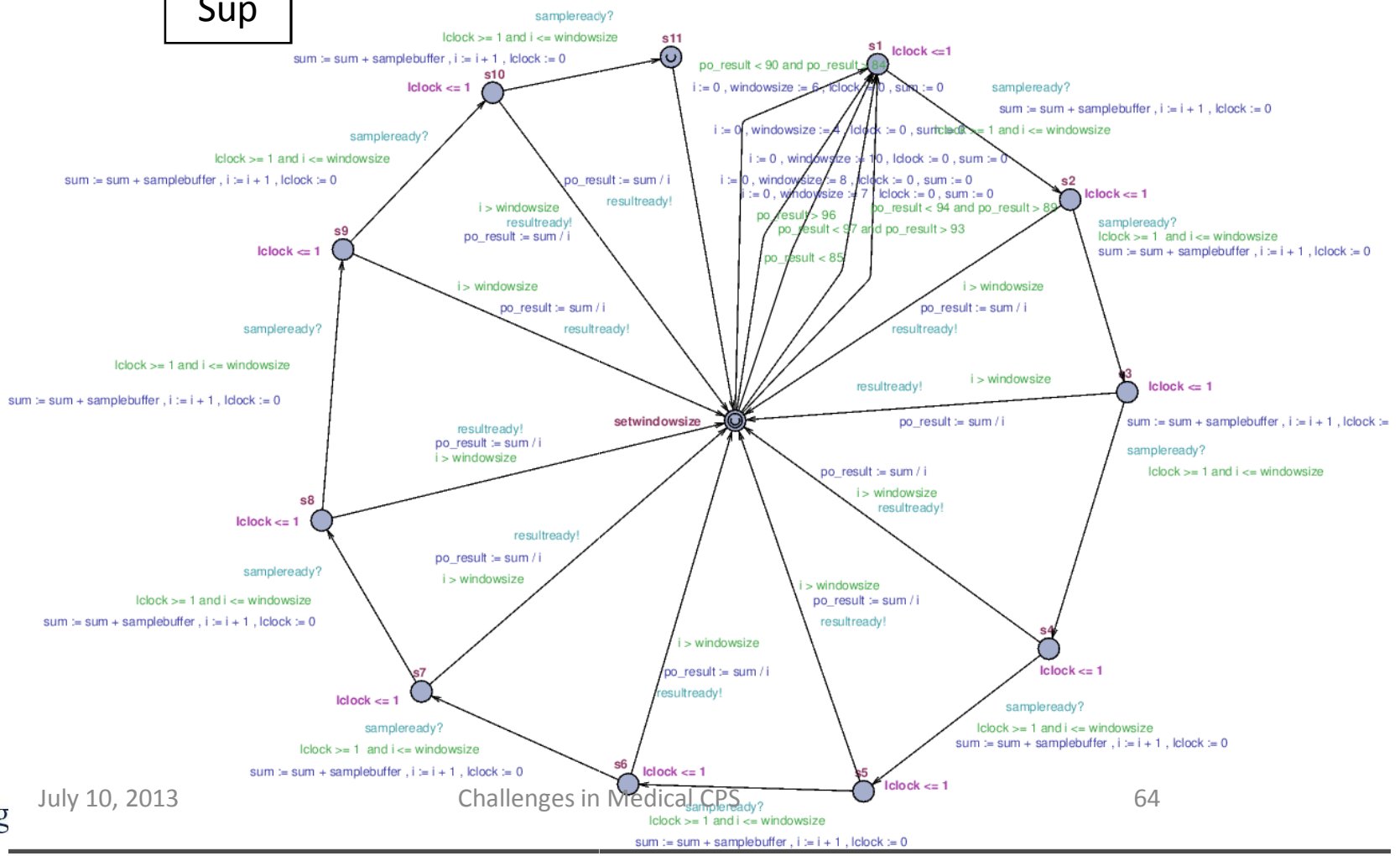
- In a more complex case, obtain using Matlab simulation



UPPAAL Model

Pulse Oximeter module:

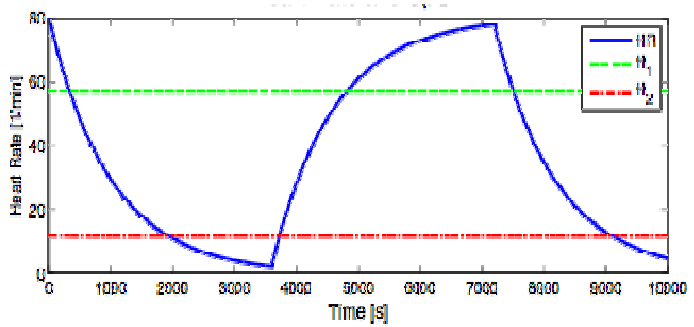
- Averages samples in a window; size of window depends on the measured value => variable delay

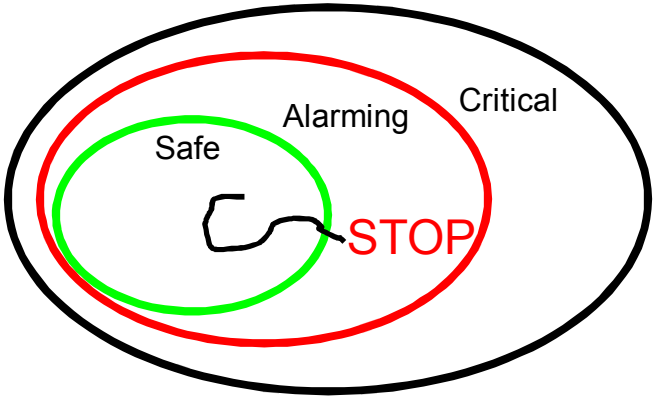


Properties verified with UPPAAL

- Once SpO2 drops below pain threshold, it eventually goes back up

  A[] (samplebuffer < pain_thresh -> A <> samplebuffer >= pain_thresh)



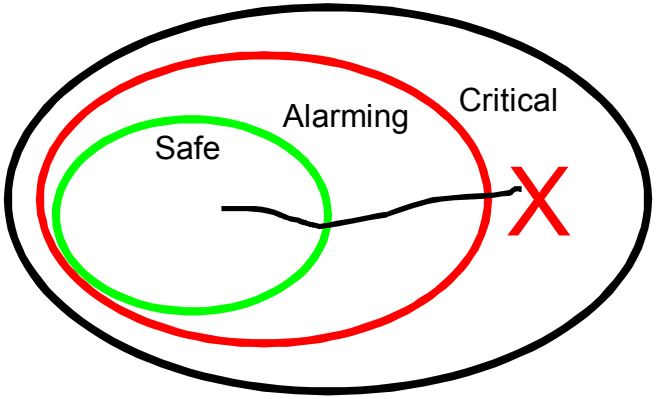


- The pump is stopped if patient enters alarming

  A[] (samplebuffer < alarm_thresh ->
  A<> (PCA.Rstopped V PCA.Bstopped)

- The patient can not go into the critical region

  A[] (samplebuffer >= critical)



Effects of unreliable network

- Problem:
  - The pump may not receive stop commands
- Solution:
  - Send a ticket: permission to run for a certain period of time
- Open-loop stability
  - We need to determine how long the pump can run without endangering the patient

$$\Delta t_{safe} \leq \tilde{t}_{safe} = \frac{1}{||\tilde{\mathbf{A}}||} \ln \left(\frac{|H_2^{\mathrm{SpO}_2} - h_{cur}|/\mathrm{SpO}_{2\,gain}}{||\tilde{\mathbf{C}}|| \cdot \left(||\tilde{x}_0|| + \frac{||\tilde{\mathbf{B}} u_i||}{||\mathbf{A}_{min}||} \right)} + 1 \right)$$

Is the Patient Safe? Is the Patient Happy?

- We have proved safety with respect to a model
- One of the risks of model-based development:
  - How good is my model?
- There usually is some agreement on the model
  - Less agreement on parameter ranges
- Narrow parameter ranges => some patients do not fit the model
- Wide parameter ranges => less effective model
  - Pump will shut down too soon for most patients

Model-Carrying Patients

- Personalized modeling is the goal
- Adaptive control is not the answer
  - Can you overdose just a little to test sensitivity?!
- Gradual system identification?
  - Perform and refine over time
  - Store model parameters in health records
  - Load the model into the controller during setup
- Just dreaming aloud…

Discussion

- Safety interlock vs. “true” closed loop control
  - The interlock only turns off the pump
    - Clinician determines operation of the pump
- Interlocks require a default safe action
  - Stopping the pump assumed safe for pain control
  - Insulin control does not have a safe action
- There is hope
  - A model of Type I diabetes has been approved for *in silico* pre-clinical trials in 2008

Summary

- Medical CPS offers a distinct set of challenges
- Lots of open problems, lots of opportunities
- It is critical to have clinicians on your team
  - Establishing a dialog is a long and painful process