CIS 4410: Pacemaker Project Demo

By Shraav Bhat and Maxwell Stone

Outline

UPPAAL Model: Pacemaker

Case 1: Heart requires pacing

- XV >= LRL, heart has not produced sense within lower rate limit interval
- Pacemaker intervenes

Case 2: Intrinsic beat occurs before LRL

- sense signal arrives - Pacemaker is inhibited as heart beats on own

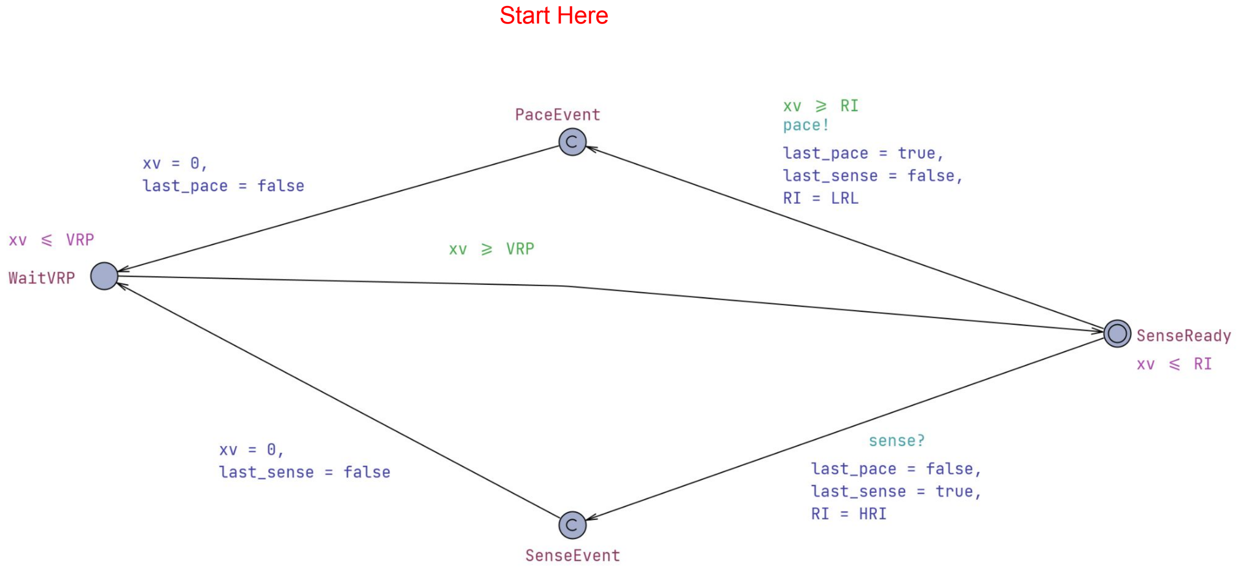
Case 3: Beat in VRP Period

- System ignores signals within the VRP

Case 4: Return to SenseReady State

a) If beat is within LRL when VRP ends, back to SenseReady

b) VRP ends and beat >= LRL we pace immediately



UPPAAL Model: Heart

Case 1: Natural (Intrinsic) Beats

- Enters Resting for atleast minIBI
- Once xh >= minIBI, back to SenseReady

Case 2: Slow Heart

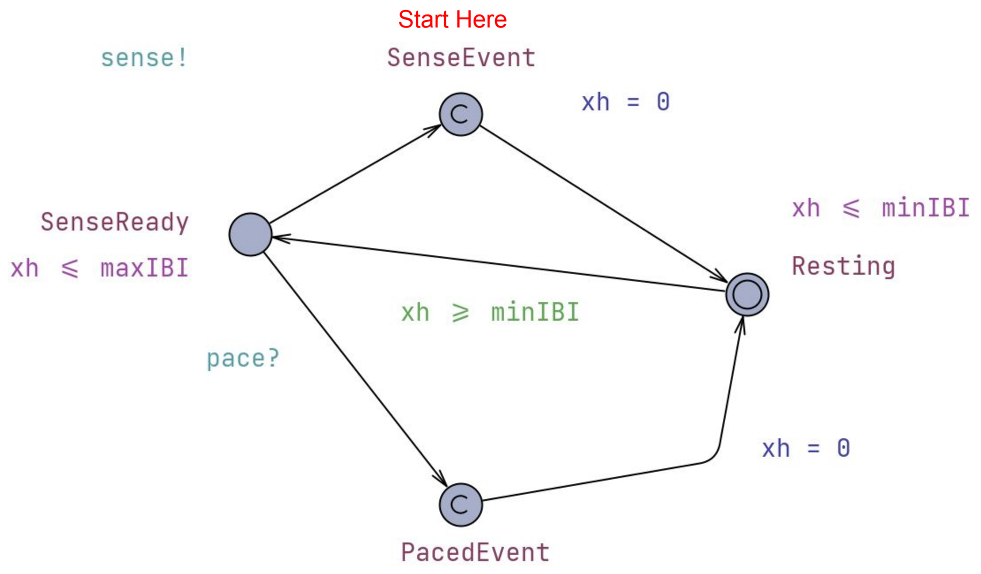
- Heart produces intrinsic beats > LRL (> 1500ms)
- If intrinsic beats come later than LRL, the pacemaker delivers a pace so the effective rate is at least 40 bpm.

Case 3: Fast Heart

- Heart faster than LRL (including very fast, e.g. minIBI 400 ms). Every sense arrives before LRL, so the pacemaker is always inhibited and does not pace, even if the intrinsic rate is above URL.

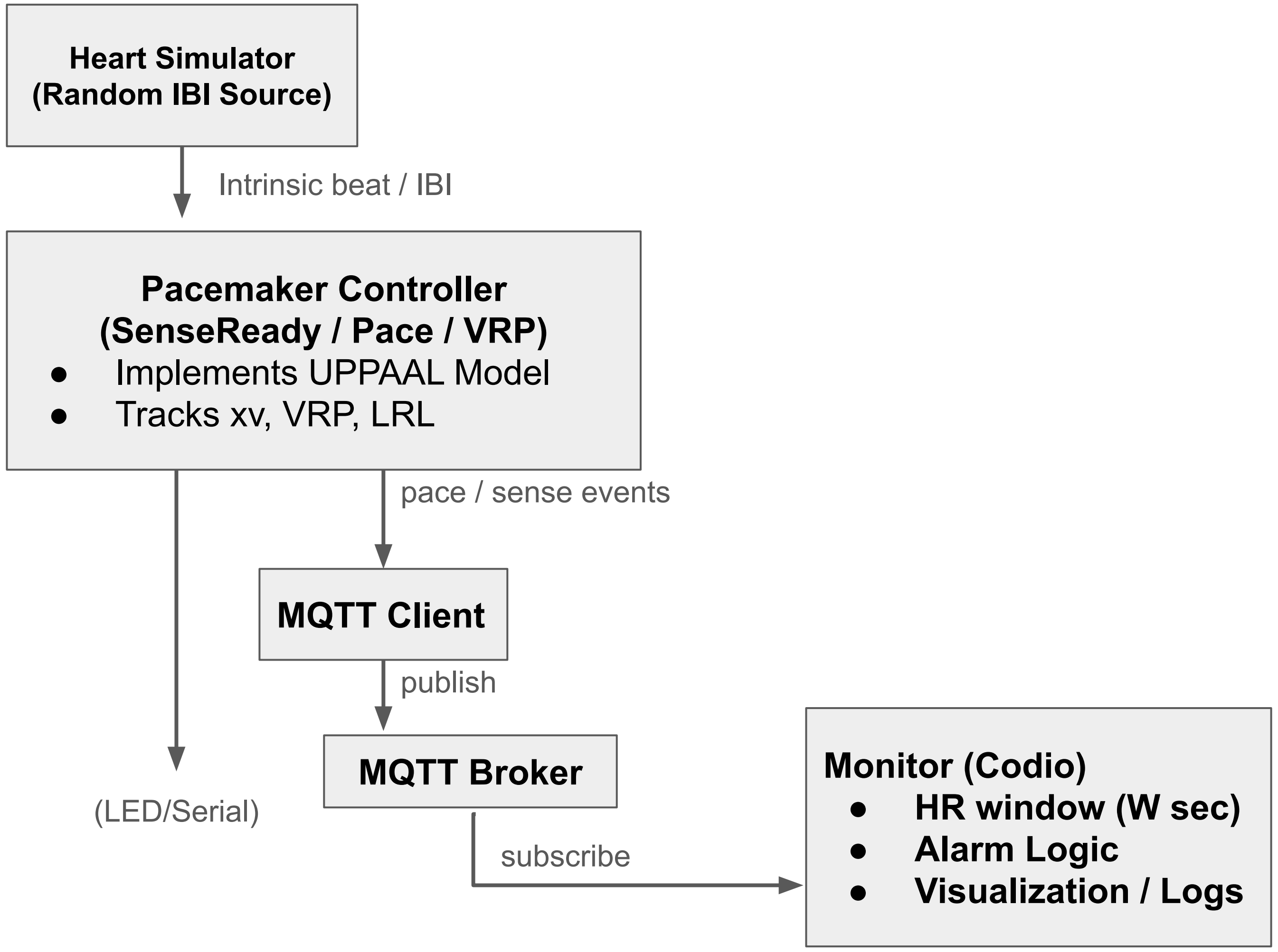
Case 4: Paced Beats

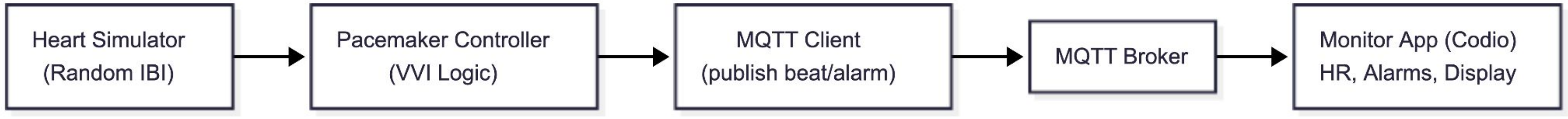
- When the pacemaker delivers a pace, it enters PaceEvent, then enters the refractory/resting state (WaitVRP), then returns to SenseReady to wait for the next intrinsic beat or pacing deadline.



Property	Result	Description
`A[] not deadlock`	✓ Pass	System never enters deadlock state
`A[] Pacemaker.WaitVRP imply Pacemaker.xv <= VRP`	✓ Pass	VRP invariant respected
`A[] (Pacemaker.xv > VRP) imply !Pacemaker.WaitVRP`	✓ Pass	Leaves VRP when timer expires
`A[] Pacemaker.xv <= LRL`	✓ Pass	Pacemaker clock bounded by LRL
`A[] Heart.xh <= maxIBI`	✓ Pass	Heart clock bounded by maxIBI
`A[] (Pacemaker.xv < URI imply !Pacemaker.PaceEvent)`	✓ Pass	No paced beat before URI
`A[] (!last_pace imply Pacemaker.xv <= RI)`	✓ Pass	Beat before LRI or HRI depending on the mode
`A[] ((!Pacemaker.WaitVRP && Heart.SenseEvent) imply Pacemaker.SenseEvent)`	✓ Pass	If the pacemaker is not in VRP and heart is at Sense event, the pacemaker must also be at sense event

High-Level System Architecture (Diagram)




Heart Simulator (Random IBI)
Pacemaker Controller (VVI Logic)
MQTT Client (publish beat/alarm)
MQTT Broker
Monitor App (Codio) HR, Alarms, Display

Implementation Architecture: Monitor/IoT structure

The controller uses **two FreeRTOS tasks**:

1. **TaskHeartPolling** (Priority 2): High-priority state machine for sensing/pacing
2. **TaskMQTT** (Priority 1): Lower-priority task for network communication and monitoring

3. **MQTT Topics**

cis441-541/heart_racer/pacemaker/heartrate: Regular metrics
cis441-541/heart_racer/pacemaker/alarm: Alarm conditions
cis441-541/heart_racer/pacemaker/status: Normal status

Alarm Conditions

Slow/Paced Heart: Triggered when >70% of beats are paced
- JSON: {"type":"SLOW_HEART", "pace_pct":X.X, "threshold":70}

Fast Heart: Triggered when average heart rate exceeds URL threshold
- JSON: {"type":"FAST_HEART", "avg_bpm":X.XX}

Real-Time Testing Results

Test 1: Normal Heart Rhythm

- Heart beats naturally at ~400-2000ms intervals (based on min and max IBI with random values in between)
- Pacemaker senses all beats successfully
- Pace percentage: <70%
- Status: NORMAL

Test 2: Slow Heart (Simulated)

Slow Heart Rate Demo

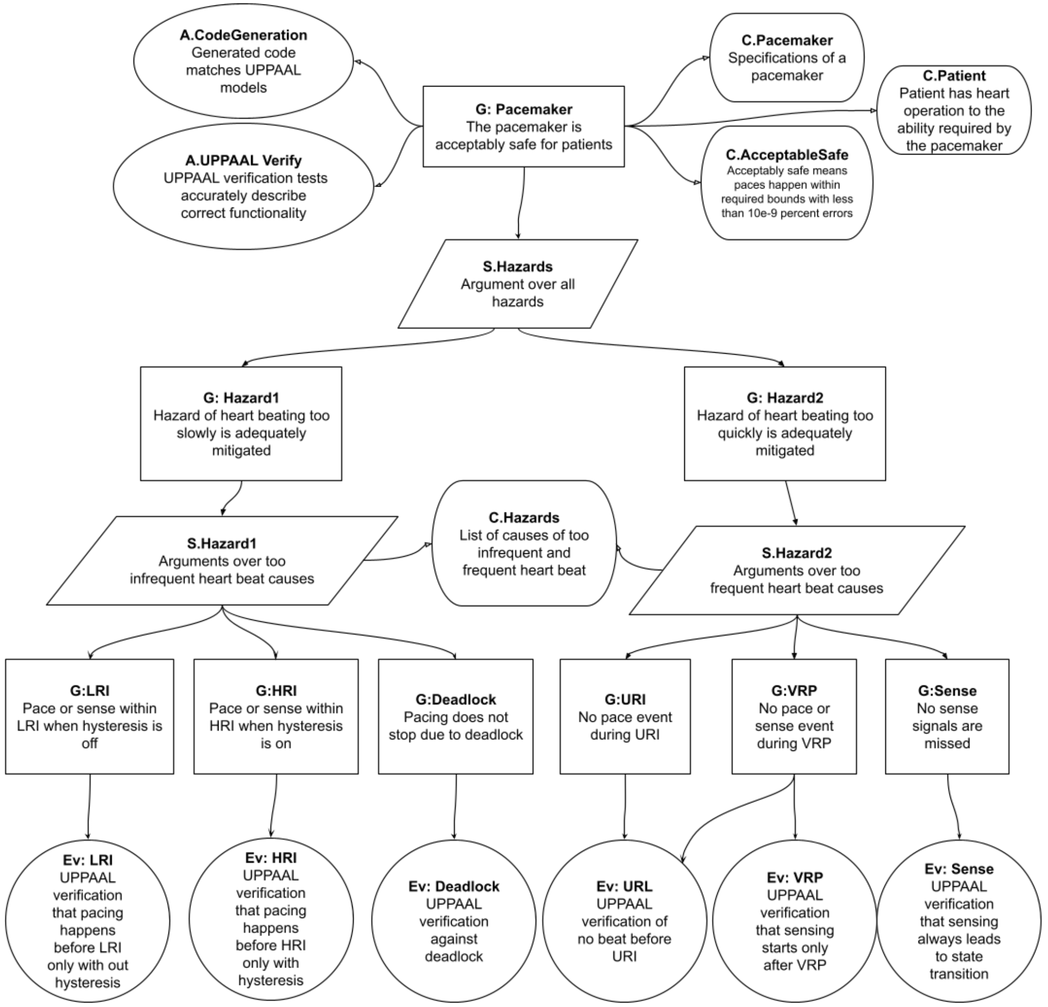
- Modified minIBI/maxIBI to 2000ms+
- Pacemaker delivers pacing pulses at LRL (1500ms)
- Pace percentage: >70%
- Alarm: SLOW_HEART triggered correctly

Test 3: Fast Heart (Simulated)

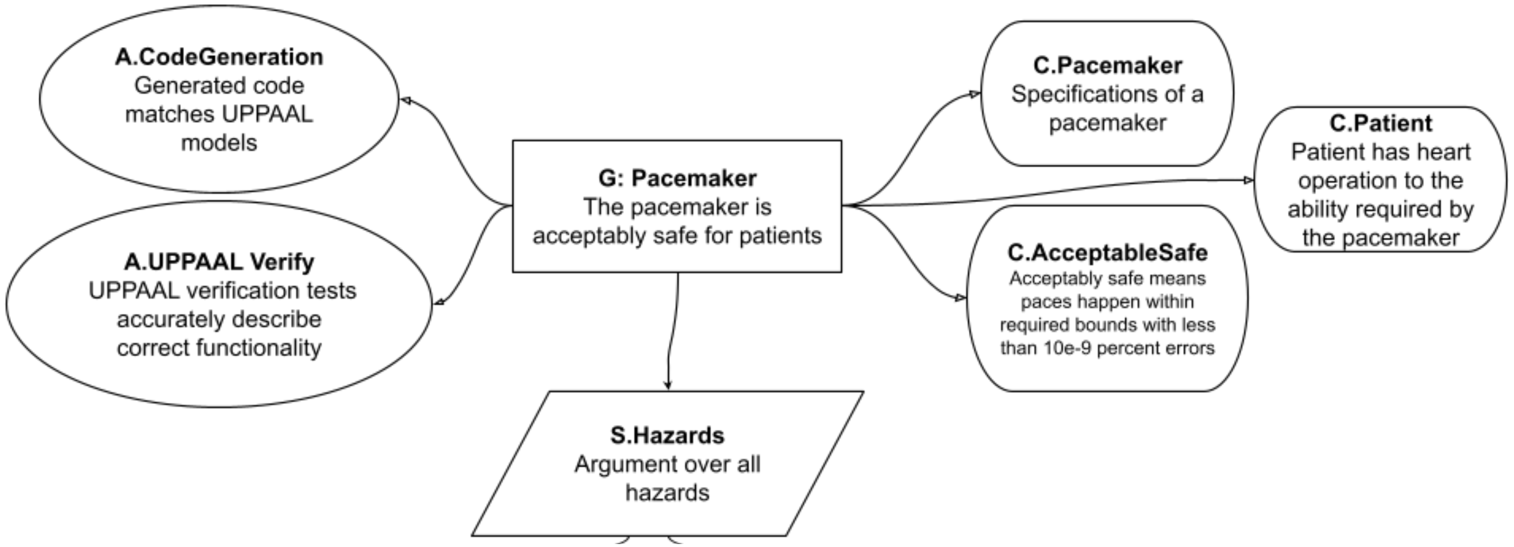
Fast Heart Rate Demo

- Modified minIBI/maxIBI to 100ms
- Average heart rate exceeds URL threshold
- Alarm: FAST_HEART triggered correctly

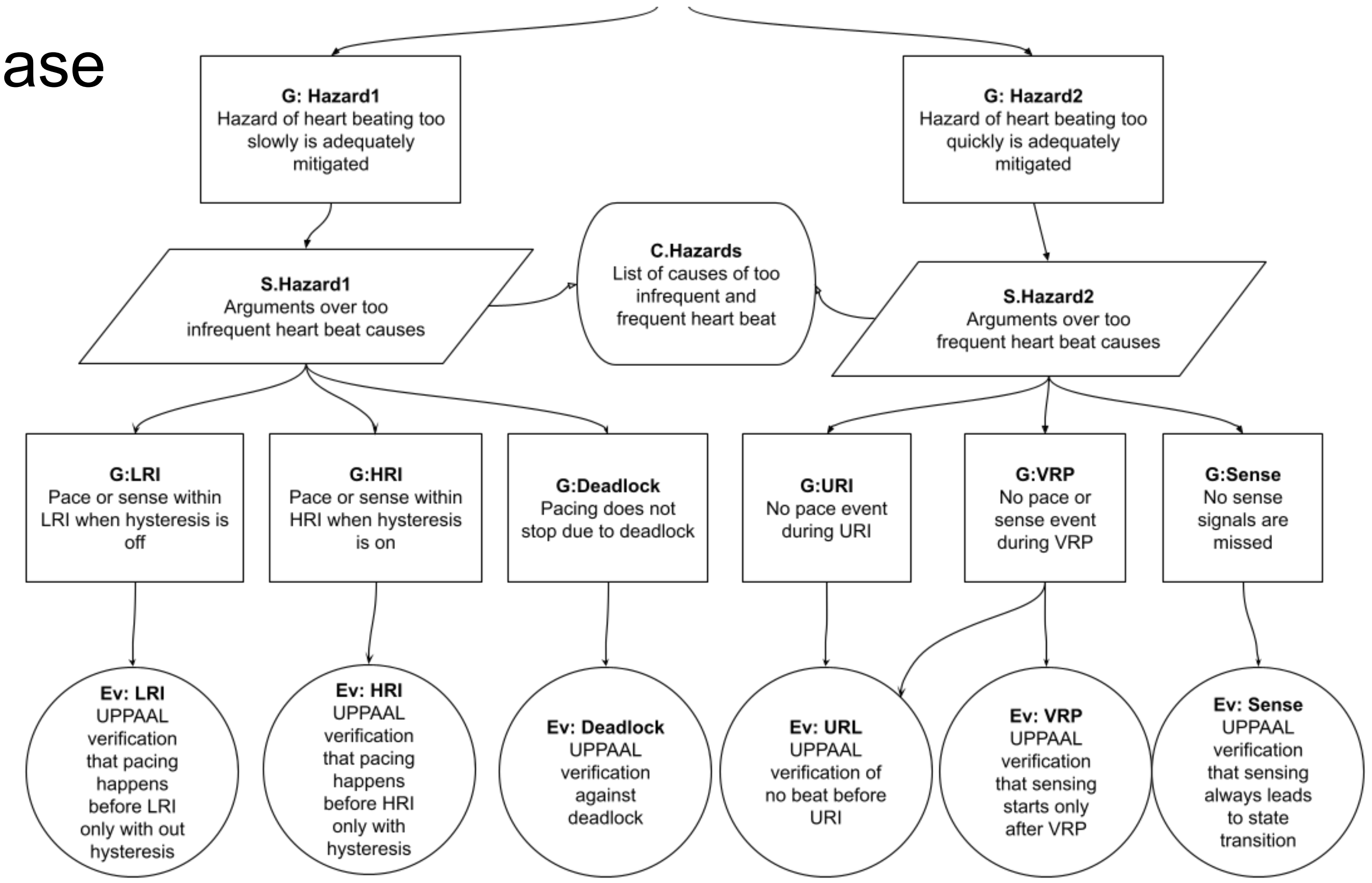
Assurance Case


A.CodeGeneration
Generated code matches UPPAAL models
A.UPPAAL Verify
UPPAAL verification tests accurately describe correct functionality
G: Pacemaker
The pacemaker is acceptably safe for patients
C.Pacemaker
Specifications of a pacemaker
C.Patient
Patient has heart operation to the ability required by the pacemaker
C.AcceptableSafe
Acceptably safe means paces happen within required bounds with less than 10e-9 percent errors
S.Hazards
Argument over all hazards
G: Hazard1
Hazard of heart beating too slowly is adequately mitigated
G: Hazard2
Hazard of heart beating too quickly is adequately mitigated
S.Hazard1
Arguments over too infrequent heart beat causes
C.Hazards
List of causes of too infrequent and frequent heart beat
S.Hazard2
Arguments over too frequent heart beat causes
G:LRI
Pace or sense within LRI when hysteresis is off
G:HRI
Pace or sense within HRI when hysteresis is on
G:Deadlock
Pacing does not stop due to deadlock
G:URI
No pace event during URI
G:VRP
No pace or sense event during VRP
G:Sense
No sense signals are missed
Ev: LRI
UPPAAL verification that pacing happens before LRI only with out hysteresis
Ev: HRI
UPPAAL verification that pacing happens before HRI only with hysteresis
Ev: Deadlock
UPPAAL verification against deadlock
Ev: URL
UPPAAL verification of no beat before URI
Ev: VRP
UPPAAL verification that sensing starts only after VRP
Ev: Sense
UPPAAL verification that sensing always leads to state transition

Assurance Case


A.CodeGeneration
Generated code matches UPPAAL models
A.UPPAAL Verify
UPPAAL verification tests accurately describe correct functionality
G: Pacemaker
The pacemaker is acceptably safe for patients
C.Pacemaker
Specifications of a pacemaker
C.Patient
Patient has heart operation to the ability required by the pacemaker
C.AcceptableSafe
Acceptably safe means paces happen within required bounds with less than 10e-9 percent errors
S.Hazards
Argument over all hazards

Assurance Case


G: Hazard1
Hazard of heart beating too slowly is adequately mitigated
G: Hazard2
Hazard of heart beating too quickly is adequately mitigated
S.Hazard1
Arguments over too infrequent heart beat causes
C.Hazards
List of causes of too infrequent and frequent heart beat
S.Hazard2
Arguments over too frequent heart beat causes
G:LRI
Pace or sense within LRI when hysteresis is off
G:HRI
Pace or sense within HRI when hysteresis is on
G:Deadlock
Pacing does not stop due to deadlock
G:URI
No pace event during URI
G:VRP
No pace or sense event during VRP
G:Sense
No sense signals are missed
Ev: LRI
UPPAAL verification that pacing happens before LRI only with out hysteresis
Ev: HRI
UPPAAL verification that pacing happens before HRI only with hysteresis
Ev: Deadlock
UPPAAL verification against deadlock
Ev: URL
UPPAAL verification of no beat before URI
Ev: VRP
UPPAAL verification that sensing starts only after VRP
Ev: Sense
UPPAAL verification that sensing always leads to state transition

Confidence Argument

Evidence-Confidence

Independently verified UPPAAL properties (assumptions checked by TA at earlier milestones)

Test cases cover partitioned timing bounds.

Context-Confidence

Hearts can beat too fast or too slow, and a pacemaker should fix the beating of a heart beating too slow, while also not exacerbating fast heart rates.

A pacemaker installed in a human body should perform reliable and correctly in its duration

Inference-Confidence

To have a safe pacemaker, we identified all relevant hazards, which include both extrema of heart beat patterns

To mitigate all relevant hazards, we identified all relevant failure points corresponding to these hazards

Demo