Approaches to the Pacemaker Challenge problem

John.Fitzgerald@ncl.ac.uk

Newcastle University

Work with Hugo Macedo (Minho), Peter Gorm Larsen (IHA), Marcel Oliveira & Artur Gomes (Rio Grande do Norte)

VSRnet Workshop at ABZ 2008, 15 September 2008

Approaches to the Pacemaker Challenge

- Background: a little cardiology
- The Pacemaker Challenge
- Work so far:
  - In Z: Gomes and Oliveira [GO08]
  - In VDM: Macedo, Larsen and Fitzgerald [MLF08]
- Future Work, and a Call to Participate!

Background: the natural pacemakers

I am not a cardiologist!

Blood flows into atria, to ventricles and out again.

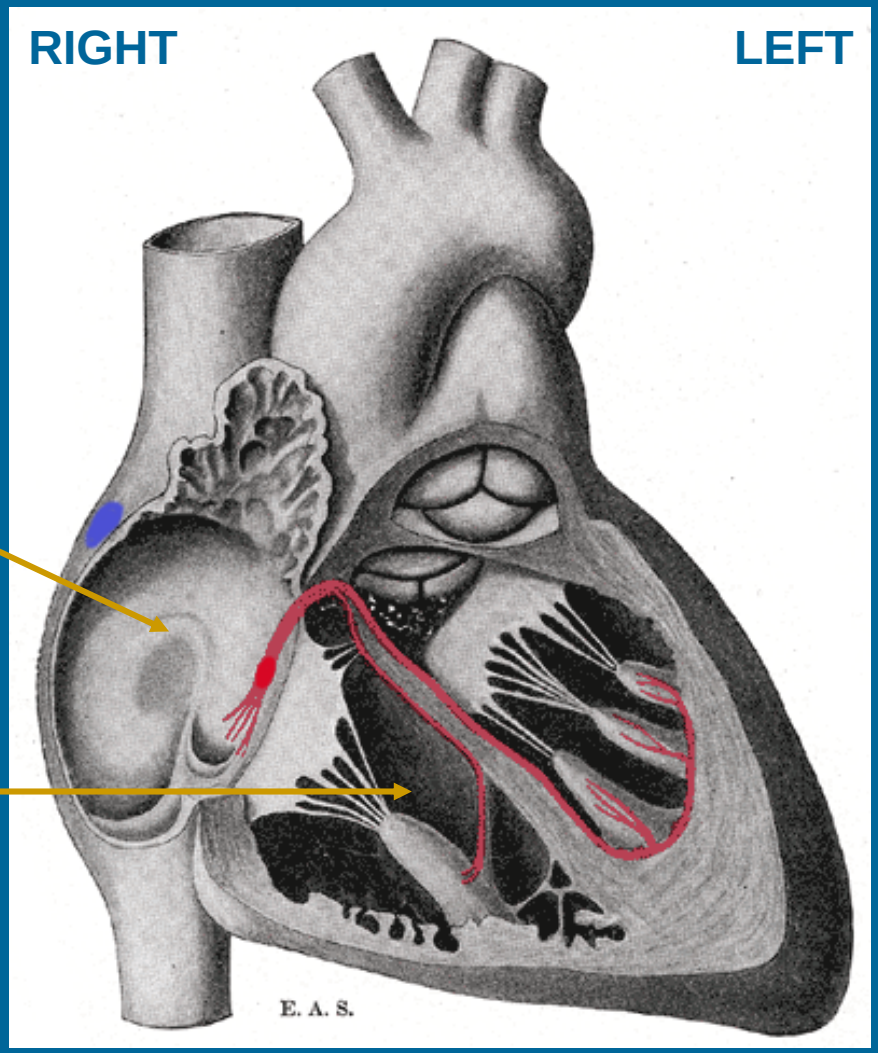


Image of Bundle of His, from Gray's Anatomy 1918)

Sino-Atrial (SA Node). Cells depolarise, creating action potentials.

Atrial muscle contracts

Signal reaches …

Atrio-Ventricular (AV Node). “Secondary Pacemaker”

Bundle of His

Reaches Ventricular walls, and the ventricular muscles contract.

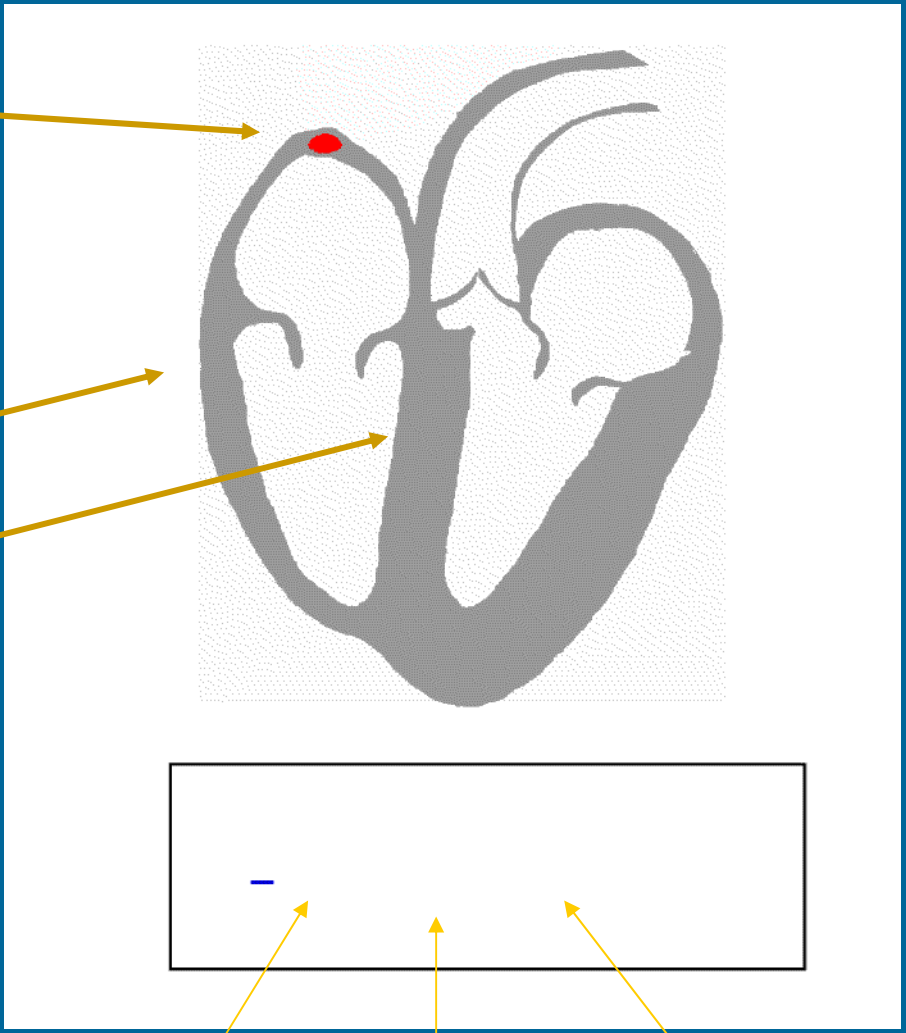


Image: Prinzip der EKG-Darstellung, Wikipedia Commons

Background: the natural pacemakers

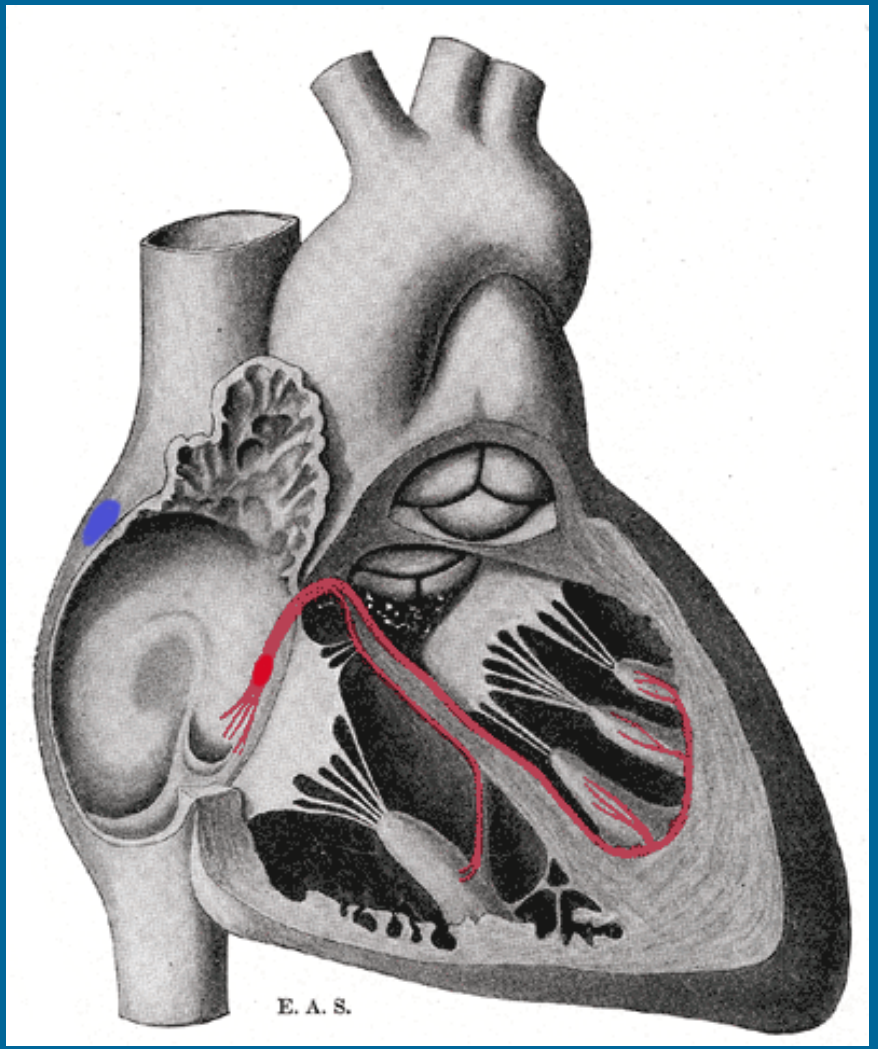
Failures include:

- Conduction disturbances (heart block): SA to AV or after the AV.
- Arrhythmia
- Slow SA node

(bradycardia and tachycardia)

Different pacing modes for different conditions, e.g.

- Regular pace of a ventricle
- Pace of the ventricle in response to a sensed AV signal
- Inhibit a pace in response to a detected signal



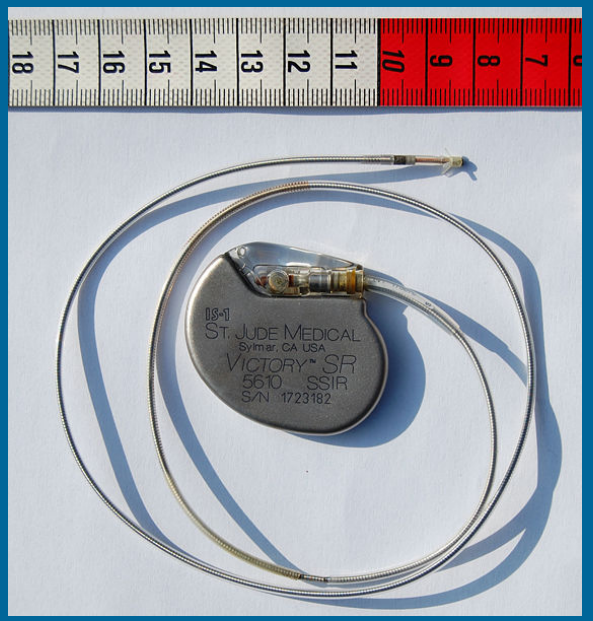
Background: artificial pacemakers

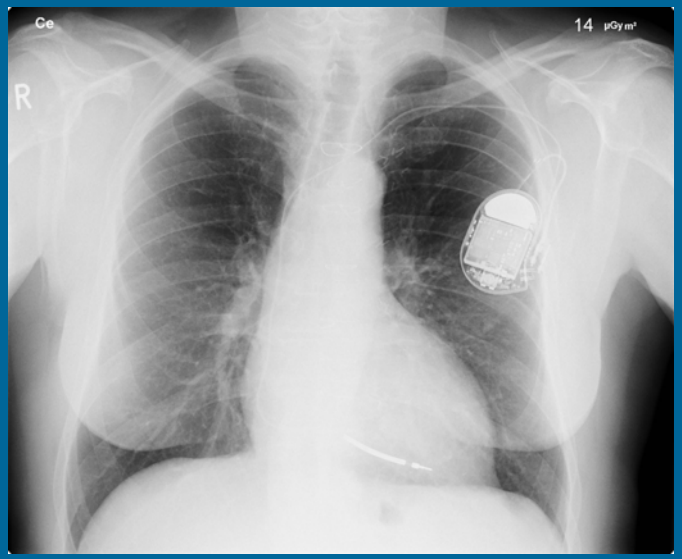
Small implanted device

Internal battery

1-2-3 leads (biploar)

10-15 years





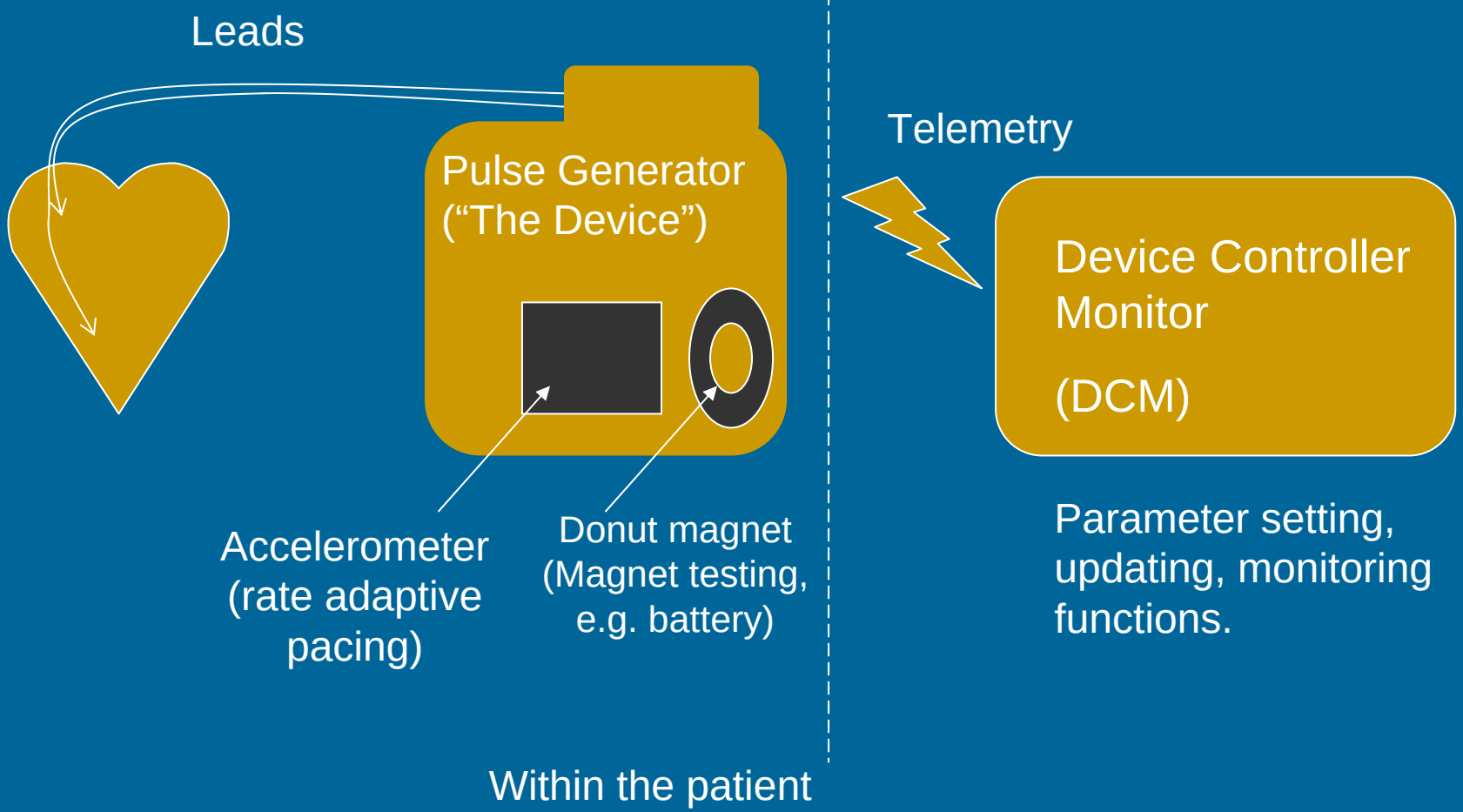
Lead passed through a vein to the right ventricle or atrium.

Device is implanted between skin and chest wall.

Modes and parameters configured just after implantation.

Image: Pacemaker image by Steven Fruitsmaak; X-Ray image; both Wikipedia Commons, 2007.

Background: artificial pacemakers



The Pacemaker Challenge

- Software is increasingly significant in medical devices (US FDA, UK MHRA)
- How can our formal techniques aid certification as well as design and code quality?
- North American Software Certification Consortium
- McMaster University (Maibaum, Lawford and Wassyng)
- SCORE Programming Competition at ICSE

The Pacemaker Challenge

- Challenge revolves round a requirements document.
- Participants invited to contribute partial or complete developments.
- An artificial certification framework to be created.
- A reference platform has been developed.
- *We're free to contribute in any area. There are no rules (yet!)*

The Pacemaker Challenge

- Requirements Document (Boston Scientific)
- 35 pages, informal natural language (English) and tables
- Main areas:
  - System: DCM, leads, pacing pulse, brady modes and state.
  - Diagnostics: monitoring, ECGs etc.
  - Bradycardia therapy: definition of user-programmable parameters (e.g. rate limits, delays).

The Pacemaker Challenge

	I	II	III	IV (optional)
Category	Chambers Paced	Chambers Sensed	Response to Sensing	Rate Modulation
Code	O – None A – Atrium V – Ventricle D – Dual	O – None A – Atrium V – Ventricle D – Dual	O – None T – Triggered I – Inhibited D – Tracked	R – Rate Modulation

- Objective of the Pulse Generator is to maintain AV synchrony
- 23 programmable pacing modes, e.g.
  - VOO: ventricle paced, no sensing (and no response to sensing)
  - VVI: ventricle paced and sensed. Reaction to sensing a QRS is to inhibit the pace.
  - AAI: atrium paced, atrium sensed. Reaction to a sensed P is to inhibit the pace.

The Pacemaker Challenge

	I	II	III	IV (optional)
Category	Chambers Paced	Chambers Sensed	Response to Sensing	Rate Modulation
Code	O – None A – Atrium V – Ventricle D – Dual	O – None A – Atrium V – Ventricle D – Dual	O – None T – Triggered I – Inhibited D – Tracked	R – Rate Modulation

- Objective of the Pulse Generator is to maintain AV synchrony
- 23 programmable pacing modes, e.g.
  - DDD: both chambers paced and sensed. Sensed P and QRS can inhibit a pace, sensed P can trigger a ventricular pace.
  - XXXR: Mode XXX with rate modulation (based on accelerometer input).

The Pacemaker Challenge

	Range	Inc.	Nominal	Tol.
Lower Rate Limit	30-50 ppm 50-90 ppm 90-175 ppm	5 ppm 1 ppm 5 ppm	60 ppm	±8 ms
Upper Rate Limit	50-175 ppm	5 ppm	120 ppm	±8 ms
Maximum Sensor Rate	50-175 ppm	5 ppm	120 ppm	±4ms
Fixed AV Delay	70-300 ms	10 ms	150 ms	±8 ms
Dynamic AV Delay	Off, On	—	Off	—
Minimum Dynamic AV Delay	30-100 ms	10 ms	50 ms	
Sensed AV Delay Offset	Off, -10 to -100 ms	-10 ms	Off	±1 ms
A or V Pulse Amplitude Regulated	Off, 0.5-3.2V 3.5-7.0 V	0.1V 0.5V	3.5V	±12%

25 programmable parameters

4 measured parameters(lead impedance, P and R wave measurements, battery power).

Two Approaches: Z

- Artur Gomes and Marcel Oliveira [GO08]
- A classical Z approach: system (moding and state requirements)
- Reasoning using ProofPower Z

Two Approaches: Z

LRL

lower_rate_limit : **N** *(*ppm*)*

inc_lower_rate_limit : **N** *(*ms*)*

tol_lower_rate_limit : **N** *(*ms*)*

$lower\_rate\_limit \in 30..175;$

$(30 \leq lower\_rate\_limit < 50) \Rightarrow (inc\_lower\_rate\_limit = 5)$

$\wedge\ (50 \leq lower\_rate\_limit < 90) \Rightarrow (inc\_lower\_rate\_limit = 1)$

$\wedge\ (90 \leq lower\_rate\_limit \leq 175) \Rightarrow (inc\_lower\_rate\_limit = 5);$

$tol\_lower\_rate\_limit = 8$

Two Approaches: Z

SWITCH ::= ON | OFF

CHAMBERS ::= C_NONE | ATRIUM | VENTRICLE | C_DUAL

RESPONSE ::= R_NONE | TRIGGERED | INHIBITED | TRACKED

BOM

switch : SWITCH;

chambers_paced : CHAMBERS;

chambers_sensed : CHAMBERS;

response_to_sensing : RESPONSE;

rate_modulation : **B**

Two Approaches: Z

DDDR

BOM

---

switch = ON;

chambers_paced = C_DUAL;

chambers_sensed = TRACKED;

rate_modulation = TRUE

Two Approaches: Z

Over 170 schemas.

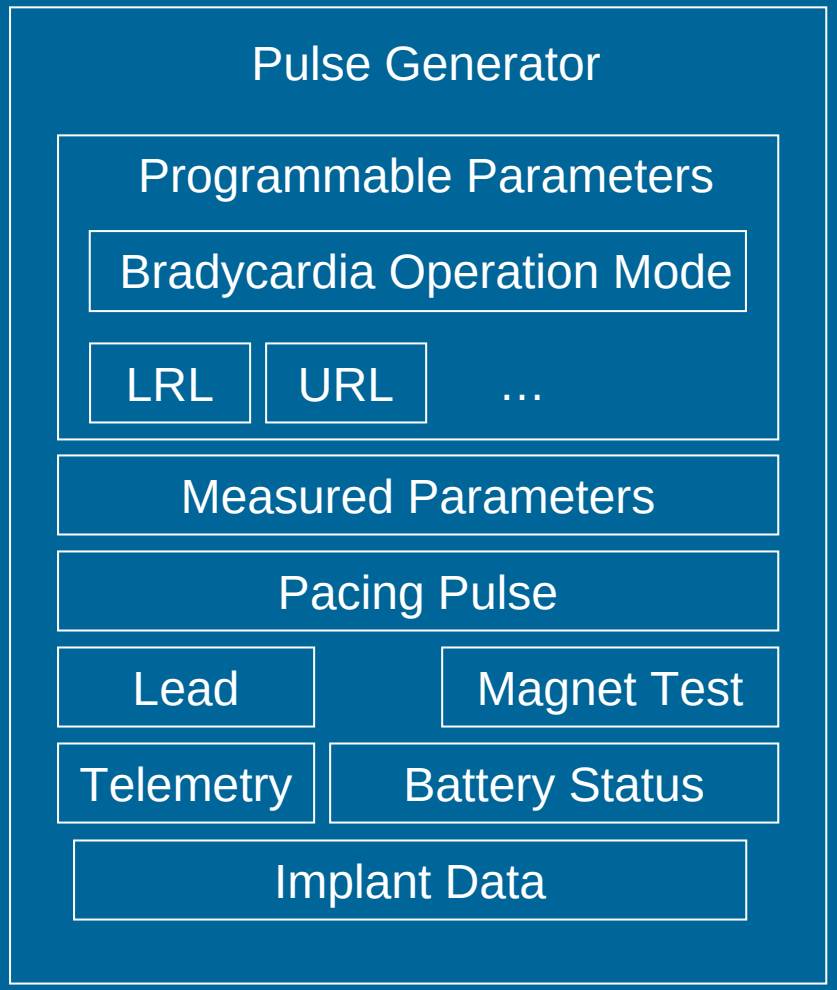
Key decisions in structuring:

- modularisation of brady. operating modes
- inclusion of telemetry in pulse generator

Covers all main brady modes, focussing on consistent use of valid parameters.

Proof of initialisation theorems.

Will add responsive mode pacing, event markers etc.



Two Approaches: VDM

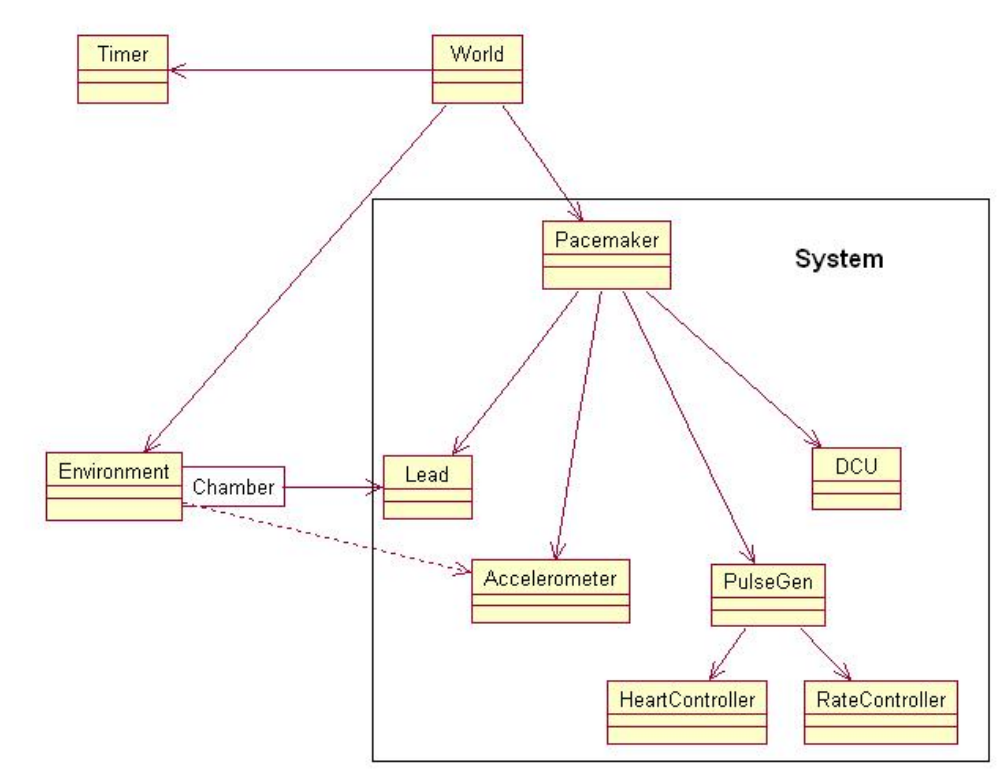
- Hugo Macedo, Peter Gorm Larsen and John Fitzgerald [MLF08, Fitz08]
- Part of a drive towards entry-level formal methods with tool support [FLS08] www.vdmportal.org/
- Purpose was to assess an incremental approach to model production [FL+07]
- For (distributed) real-time applications
- Approach was staged modelling of a subset of requirements

Two Approaches: VDM

1. Abstract VDM model defining functionality of brady modes as relations on sensed and reaction timelines.
2. Executable sequential model structured into environment and system components.
3. Executable concurrent model.
4. Executable RT model (with distribution)

Covered 8 modes and 18 of the controlling variables.

Validation by test.



Two Approaches: VDM

SenseTimeline = set of (Sense * Time);

ReactionTimeline = set of (Reaction * Time)

functions

PacemakerDOO (inp: SenseTimeline) r: ReactionTimeline

post … forall mk_(<ATRIUM>,ta) in set r &

exists mk_(<VENTRICLE>,tv) in set r & tv = ta + FixedAV);

Two Approaches: VDM

- Sequential model introduces environment/system division
- Environment class controls production of stimuli via a Leads class (lock-step)
- Concurrent model frees Environment class (but it still manages time)
- Identifies concurrency issues

Two Approaches: VDM

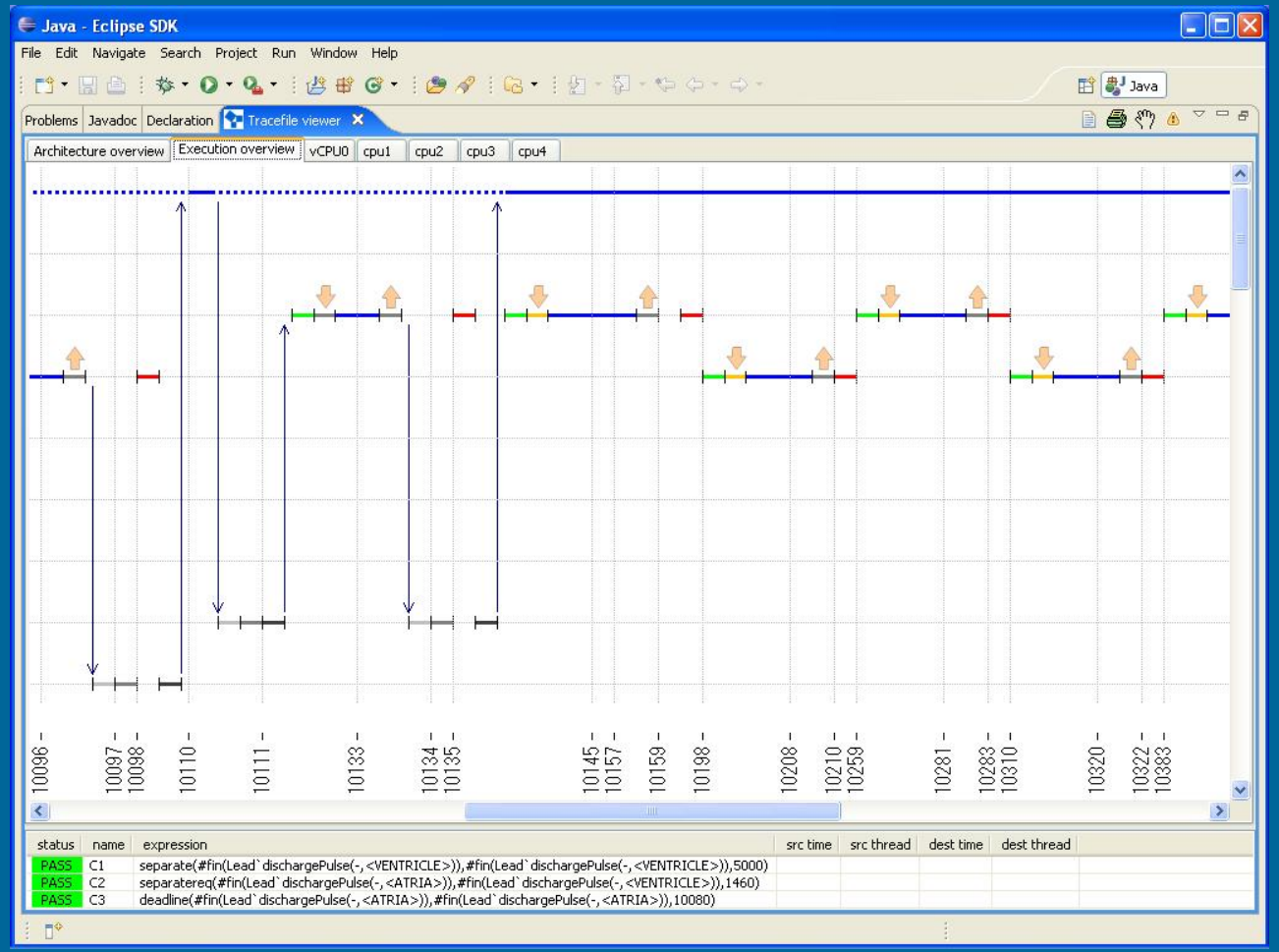
- Distributed RT model
- Threads are defined with periodicity, jitter etc.
- Time annotations (durations) model durations of particular actions.

```
dischargePulse: Pulse * Chamber ==> ()
dischargePulse(p,c) ==
        if c = <ATRIUM>
        duration(40) World`env.handleEvent(p,c,time)
```

Two Approaches: VDM

VDM tool “plugin” for Visualisation of model executions with validation conjecture checking …

RTL-like validation conjectures [FL+07]



Two Approaches: Z & VDM

- Both have identified numerous questions against requirements
  - Operating mode consistency
  - Modelling errors (race conditions)
- Complementary coverage

Future Work

- Work required (urgently!) on spec derivation from requirements
- We'll improve coverage of the models
- Proof-based validation
- Co-simulation with heart models
- Continuous/Discrete boundary
- Design of specific algorithms (e.g. rate smoothing)
- Evidence for certification

Future Work

Reference implementation platforms are available (CDN$350) from McMaster, or designs are available on line.

Pacemaker wiki:
http://sqrl.mcmaster.ca/pacemaker.htm
http://www.cas.mcmaster.ca/wiki/index.php/Pacemaker

Information Sources

PACEMAKER System Specification, Boston Scientific, 2007. Available at http://sqrl.mcmaster.ca/pacemaker.htm

[GO08] Artur Gomes and Marcel Oliveira, *Modelling the Pacemaker: early results on the pulse generator,* in *Workshop on Pilot Projects for the Grand Challenge in Verified Software* at FM 2008.

[FLS08] John Fitzgerald, Peter Gorm Larsen and Shin Sahara, *VDMTools: advances in support for formal modeling in VDM*, ACM SIGPLAN Notes 43(2), February 2008, pp. 3-11.

[Fit08] J. S. Fitzgerald, *The Grand Challenges and VDM: an update on the Pacemaker, Posix and Mondex,* in *Workshop on Pilot Projects for the Grand Challenge in Verified Software* at FM 2008.

[MLF08] H. D. Macedo, P. G. Larsen and J. S. Fitzgerald, *Incremental Development of a Distributed Real-Time Model of A Cardiac Pacing System using VDM*, in Proc. FM 2008, 15th Intl. Symp. on Formal Methods, Aabo Akademi, Finland, Springer LNCS May 2008.

[FL+07] J. S. Fitzgerald, P. G. Larsen, S. Tjell and M. Verhoef. *Validation Support for Distributed Real-Time Embedded Systems in VDM++*. in Bojan Cukic and Jing Dong (Eds.), Proc. 10th IEEE High Assurance Systems Engineering Symposium, November, 2007, Dallas, Texas, pp. 331-340.