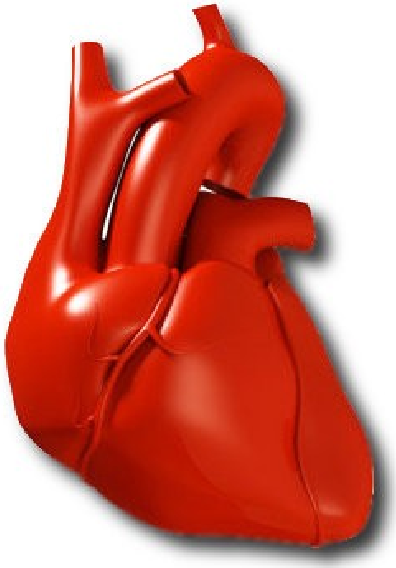
A Simple Pacemaker Implementation

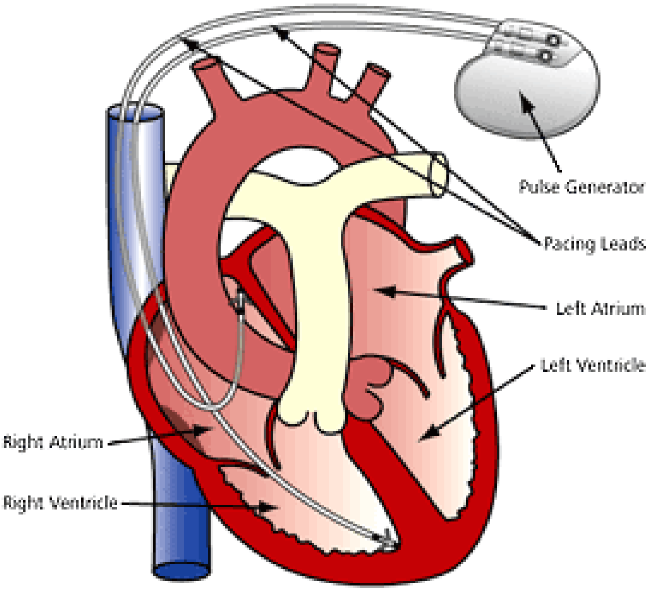


Valerio Panzica La Manna
Alfredo Motta
Andrea Tommaso Bonanno

Project Proponent: Alan Wassyng

What is a Pacemaker?

- A medical device that regulates the beating of the heart using electrical impulses to contract the heart muscles.
- The primary purpose of the pacemaker is to maintain an adequate heart rate.
- Modern pacemakers are externally programmable and allow the cardiologist to select the optimum **pacing modes** for individual patients.



Problem Statement

- Implement behavior described in the Pacemaker Requirements Document by Boston Scientific.

- Need to demonstrate:
  - **Utility :** it performs helpful actions
  - **Safety :** it does not perform harmful actions.

Function Modes

- The pacemaker function modes are described by simple mnemonics.

	I	II	III	IV(optional)
Category	Chambers Paced	Chambers Sensed	Response To Rate	Rate Modulation
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	R–Rate

- Modes implemented:
  - **AAT**: a very simple mode that "paces" the atrium every time a "sense" is detected.
  - **VVI**: a mode that paces the ventricle depending on whether there is or is not a natural ventricle sense.
  - **DDD**: a more complex mode that paces both the atrium and/or ventricle depending on atrial and ventricular senses.

Solution

- Formal specification of a subset of the natural language requirements.
  - TRIO used as the specification language.
- Analysis of the formal specification to check consistency.
  - PVS and ZOT used.
- Simulation of the pacemaker behavior.
  - Implemented in Java on a desktop platform.
- Simulation tested.

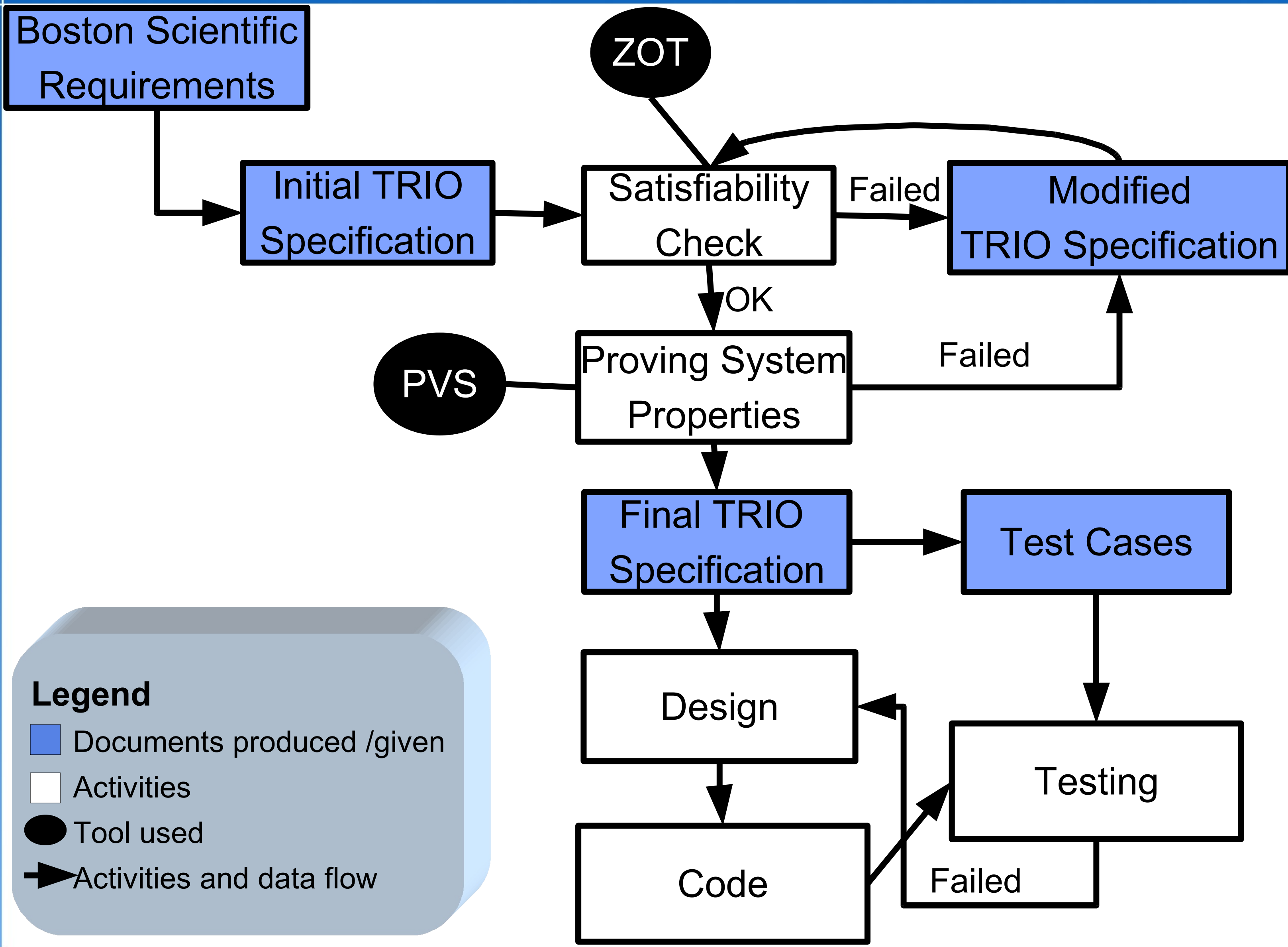
The Importance of Formal Methods

- The project is an example of:
  - A safety critical system
  - A real-time system

FORMAL METHODS

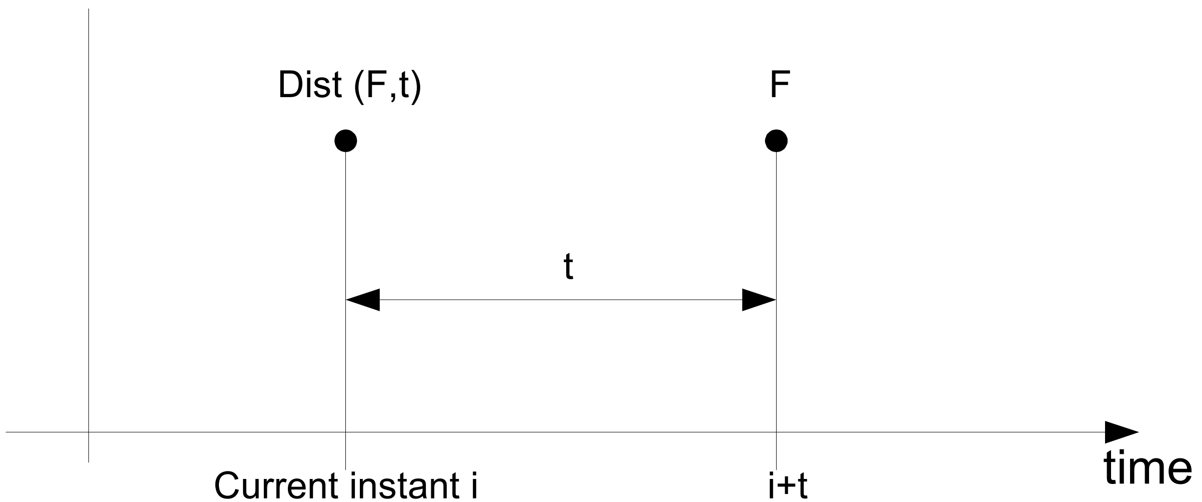
- Use of temporal first order logic to specify the behavior of the system enables us to produce test cases very easily and simplify the design.
- We were also able to prove the correctness of some properties: safety and utility.

Project Steps



TRIO

- TRIO is a Formal Language based on a metric extension of first-order temporal logic and exploits typical object-oriented features to support the managing of large, complex, and maintainable specifications.
- The basic operator Dist(F,t) specifies that F holds after/before t time instants.



TRIO Operators

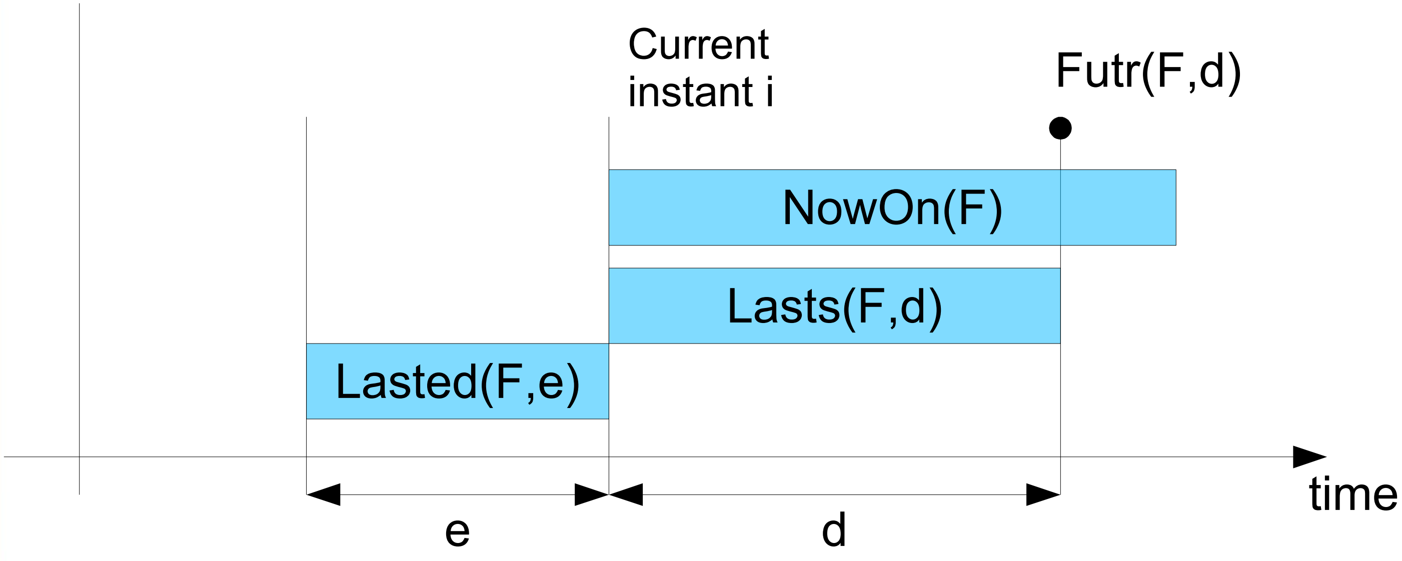
- **Futr(F, d)** ⇔ d ≥ 0 ∧ Dist(F, d)

  F will be true after a time interval of d.
- **Lasts[ee|ii|ie|ei](F, d)** ⇔ ∀d' (0<d'<d→Dist(F, d'))

  F holds over a period of length d.
- **Lasted[ee|ii|ie|ei](F, d)** ⇔ ∀d'(0<d'<d → Dist(F, -d'))

  F held over a period of length d in the past.
- **NowOn(F)** ⇔ ∃d (d>0 ∧ Lasts(F,d))

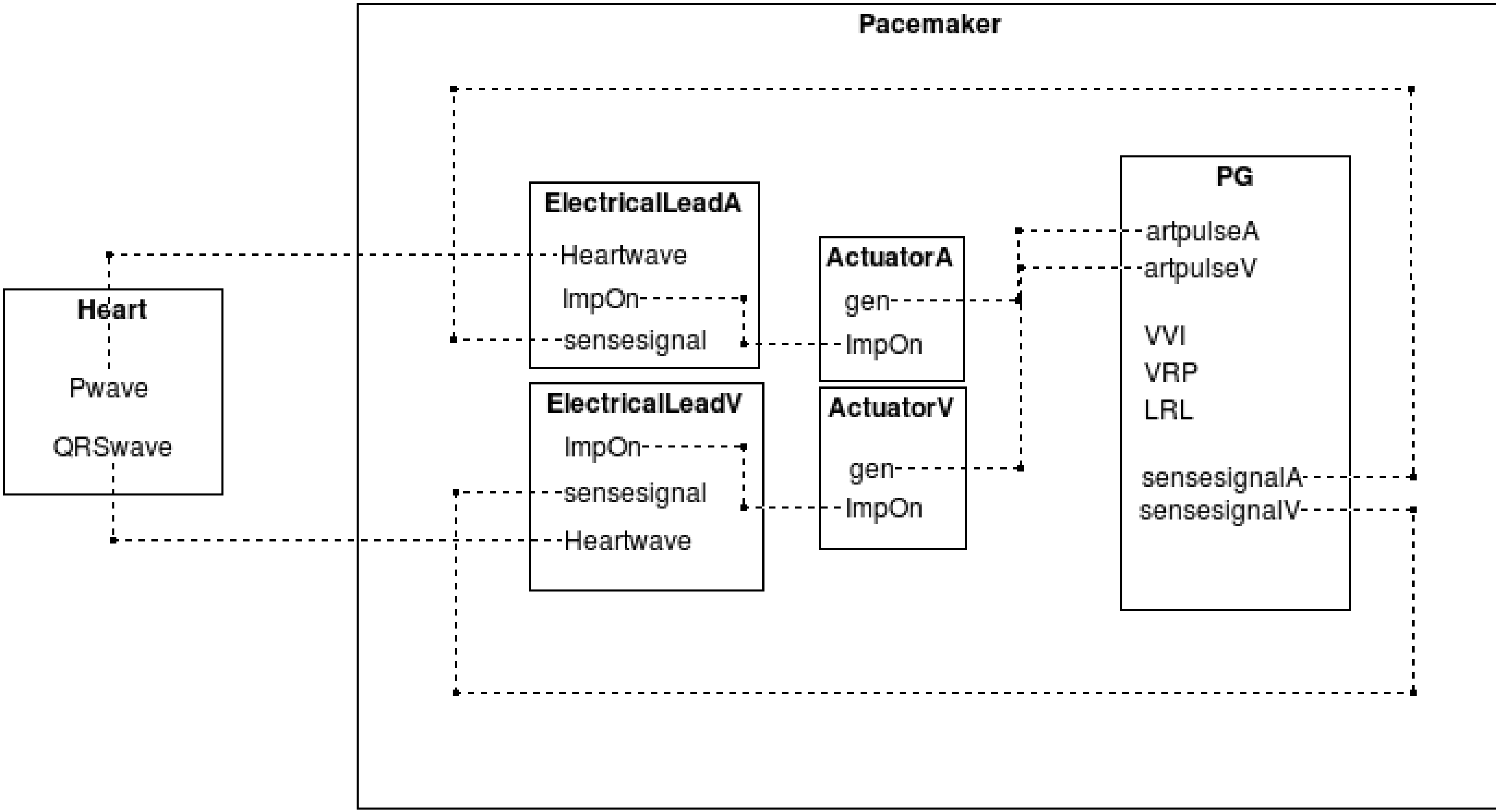
  F holds over a certain period of unspecified length.



System Components

- Boston Scientific Requirements:
  - The system consists of 3 components
    - Pulse Generator (PG)
    - Device Control Monitor (DCM)
    - Leads

- TRIO+ Modular Specification:
  - Using the concept of classes it is possible to group together sets of axioms that refer to the same component.


Pacemaker
Heart
Pwave
QRSwave
ElectricalLeadA
Heartwave
ImpOn
sensesignal
ElectricalLeadV
ImpOn
sensesignal
Heartwave
ActuatorA
gen
ImpOn
ActuatorV
gen
ImpOn
PG
artpulseA
artpulseV
VVI
VRP
LRL
sensesignalA
sensesignalV

VVI

- V: Ventricle Paced
- V: Ventricle Sensed
- I: “A sense in a chamber shall inhibit a pending pace in that chamber”

- TRIO Specification:

1) **AXIOM** Alw(sensesignalV AND NOT ignoresignalV IFF senseV)

2) **AXIOM** Alw(senseV IMPLIES NowOn(ignoresignalV))

3) **AXIOM** Alw(VVI IMPLIES (Lasted(NOT senseV,TIMEOUT) IFF artpulseV))

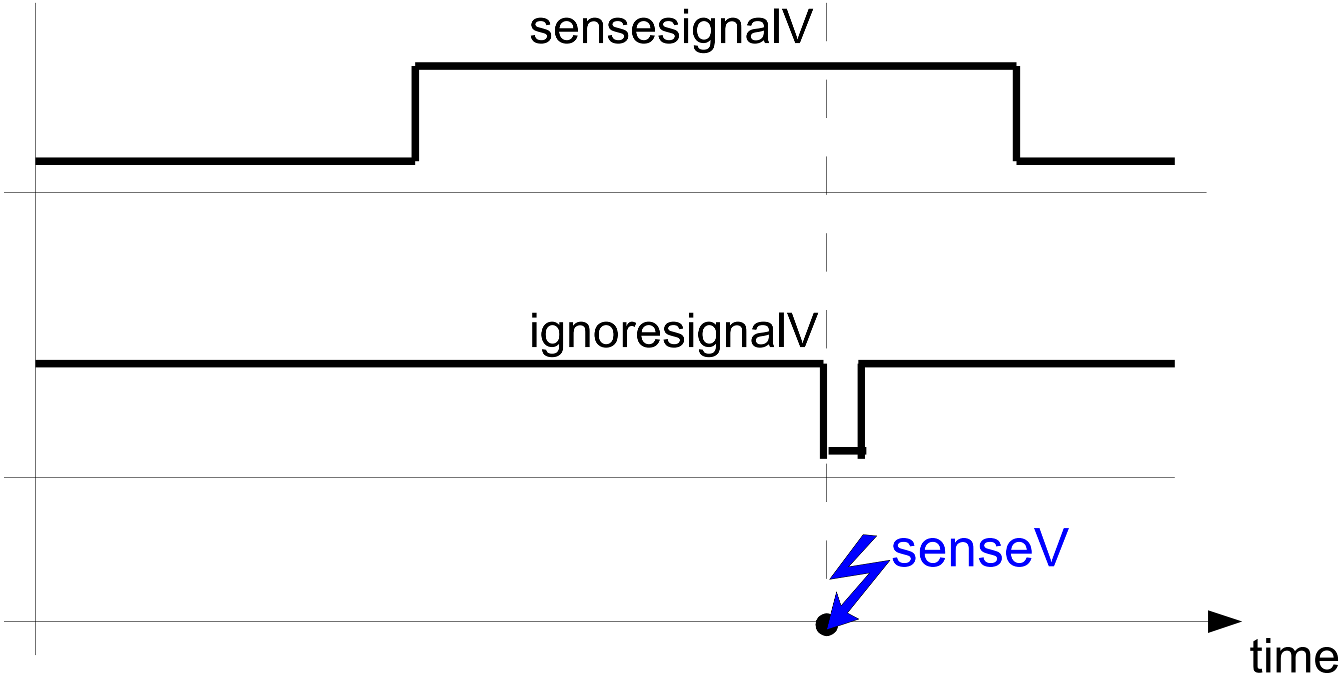
What is a ventricular event? senseV

1) AXIOM Alw(sensesignalV AND NOT ignoresignalV IFF senseV)

senseV is an event occurring when there is a signal in the ventricle and it is not ignored.

2) AXIOM Alw(senseV IMPLIES NowOn(ignoresignalV))

Detected the ventricular event senseV then ignore any signal for a certain time interval (refractory period).

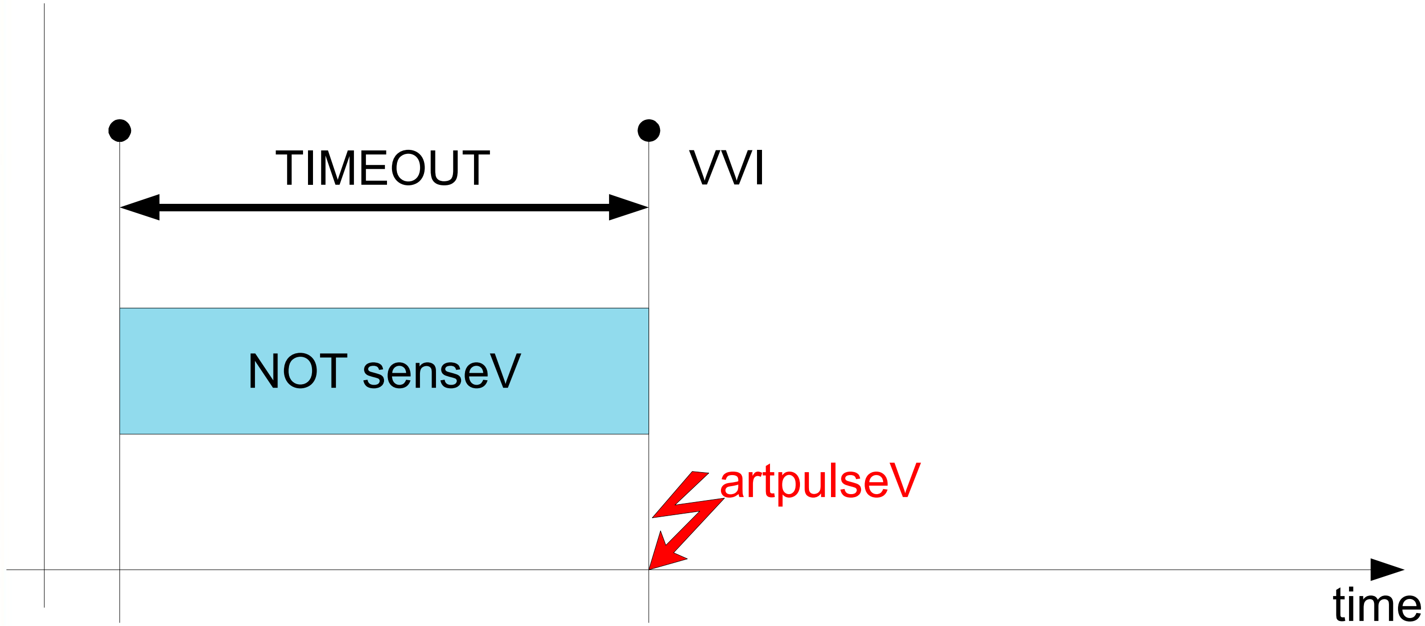


VVI

- I: “A sense in a chamber shall inhibit a pending pace in that chamber”
- TRIO Spec:

AXIOM Alw(VVI IMPLIES

(Lasted(NOT senseV,TIMEOUT) IFF artpulseV))

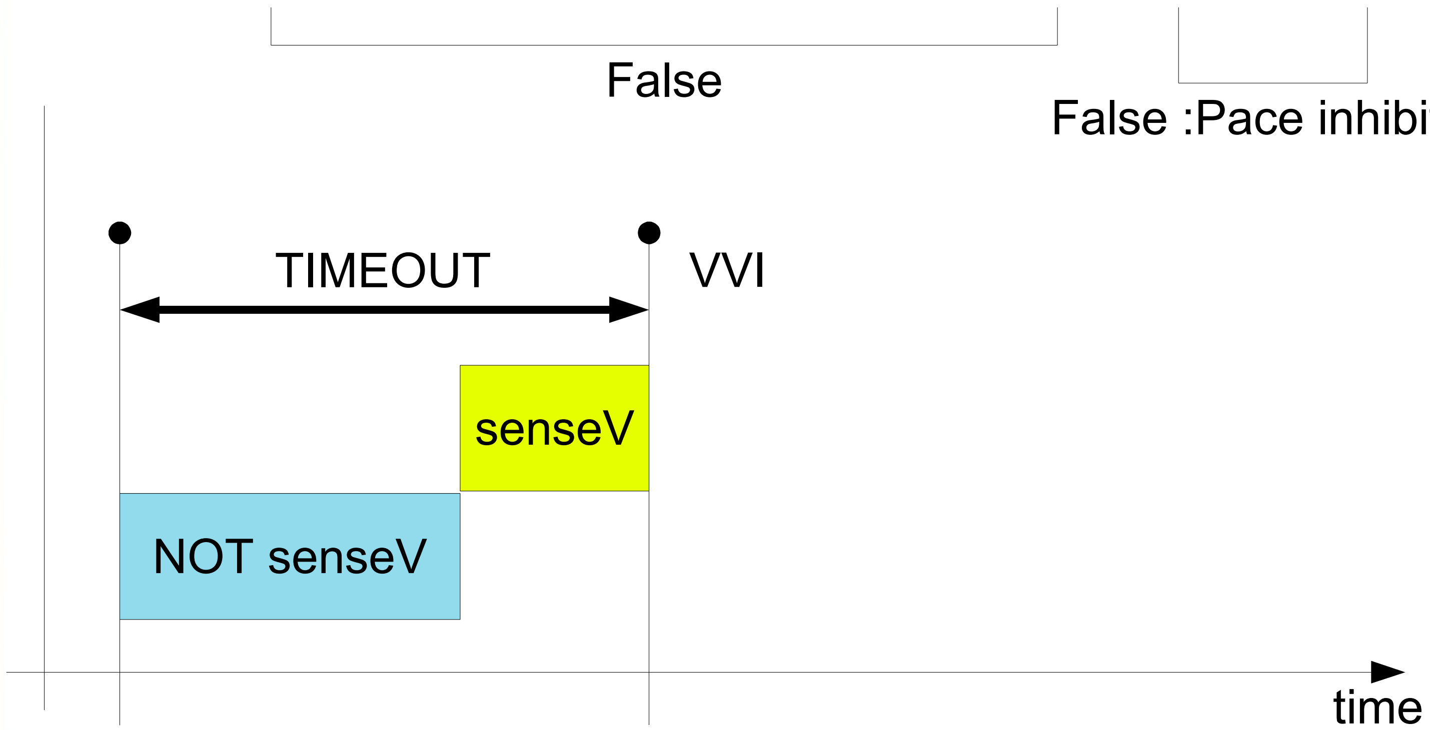


VVI

- I: “ A sense in a chamber shall inhibit a pending pace in that chamber”
- TRIO Spec:

AXIOM Alw(VVI IMPLIES

(Lasted(NOT senseV,TIMEOUT) IFF artpulseV))



ZOT: Sat Checker

- The ZOT tool is used to verify the satisfiability of the overall system TRIO axiomatization.
- If a contradiction is found, a counterexample is shown.
- Problem: The check is performed at discrete time.

↓

Not enough for the proof of crucial system properties

ZOT output

```
------ time 0 ------
  VVI

------ time 1 ------
  VVI

------ time 2 ------
  VVI

------ time 3 ------
  VVI

------ time 4 ------
  VVI

------ time 5 ------
  VVI

------ time 6 ------
  VVI

------ time 7 ------
  VVI
  NATPULSEA

------ time 8 ------
  VVI
  SENSEA
  SENSESIGNALA
  PWAVE

------ time 9 ------
  ARTPULSEV
  VVI
  IGNORESIGNALA_ARP
  SENSESIGNALA
  PWAVE

------ time 10 ------
  VVI
  SENSEV
  IGNORESIGNALA_ARP
  SENSESIGNALV
  IMPONV

------ time 11 ------
  VVI
  IGNORESIGNALV
  IGNORESIGNALA_PVARP
  SENSESIGNALV
  IMPONV

------ time 12 ------
  VVI
  IGNORESIGNALV
  IGNORESIGNALA_PVARP

------ time 13 ------
  VVI

------ time 14 ------
  VVI

------ time 15 ------
  VVI

------ time 16 ------
  VVI

------ time 17 ------
  VVI

------ time 18 ------
  VVI
  NATPULSEA

------ time 19 ------
  **LOOP**
  VVI
  SENSEA
  SENSESIGNALA
  PWAVE

------ time 20 ------
  ARTPULSEV
  VVI
  IGNORESIGNALA_ARP
  SENSESIGNALA
  PWAVE

------ time 21 ------
  VVI
  SENSEV
  IGNORESIGNALA_ARP
  SENSESIGNALV
  IMPONV
```

PVS: Proving Properties

- It is a Theorem Prover: a tool that automates some typical logical operation necessary for a formal demonstration.
- Human support required.
- Supports the TRIO Axiomatization. TVS: TRIO PVS
- When a property is proved, it holds for all the possible models even in continuous time.

↓

The property is valid

PVS: Proved Properties

- **Utility:** *If the patient Heart Rate (HR=1/RR) is not within the normal range the pacemaker has to pace the heart artificially as defined by the required LRL. Note that Timeout= 1/LRL.*

  CONJECTURE

  Alw(senseV AND RR>Timeout AND VVI AND Lastsii(VVI, Timeout) IMPLIES

  Futr(senseV, Timeout) AND Lasts(NOT senseV, Timeout))

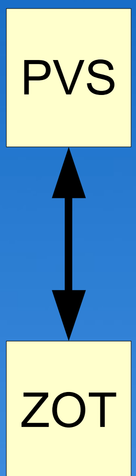
- **Safety:** *If the heart behaves normally the pacemaker does not interfere with its natural pulse.*

  CONJECTURE

  Alw(senseV AND RR<=Timeout AND VVI AND Lastsii(VVI, RR) IMPLIES

  Futr(senseV, RR) AND Lasts(NOT senseV, RR))

PVS and ZOT: Complementary Tools



- ZOT
  - Automatically checks the satisfiability of the system.
  - Produces examples useful in understanding the correctness of the axiomatization.
- PVS
  - Used to prove the target properties.
  - Forces a manual process that clarifies which axiom is not correct and why not.

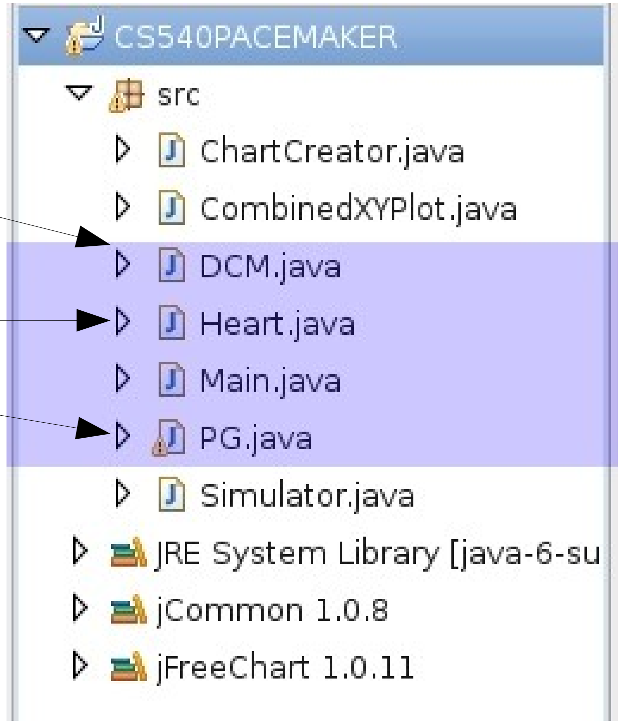
Every time a new axiom is introduced, this validation process is repeated.

Java Simulator

- Simulation is needed to:
  - Have a visual verification of the Pacemaker behavior, validating the simulated results with the expected one in the analysis steps.
  - Develop a visual understanding of the different function modes.
  - Demonstrate how the formal approach we used is well suited to rapidly produce a software prototype.

Java Simulator

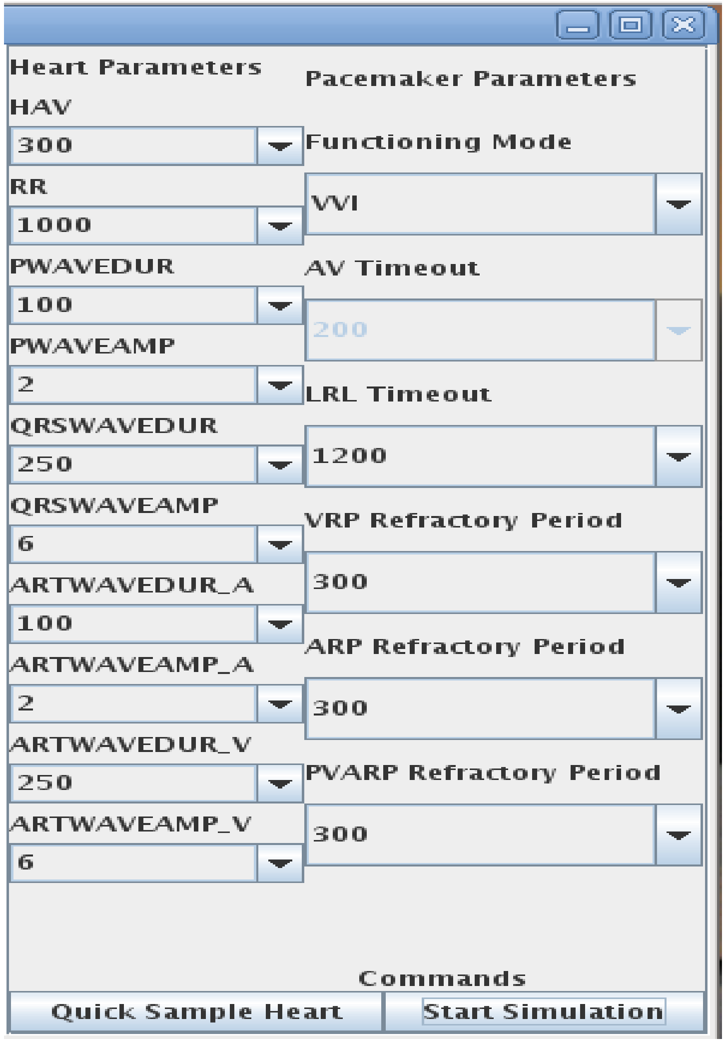
- Java classes represent all the Pacemaker modules:
  - Device Control Monitor, to set Pacemaker parameters.
  - Heart Behavior (not presented in the BS Requirements).
  - Pulse Generator set in the appropriate functioning mode.
  - Electrocardiogram as the output of the simulation.



- TRIO axioms are manually translated into Java methods.

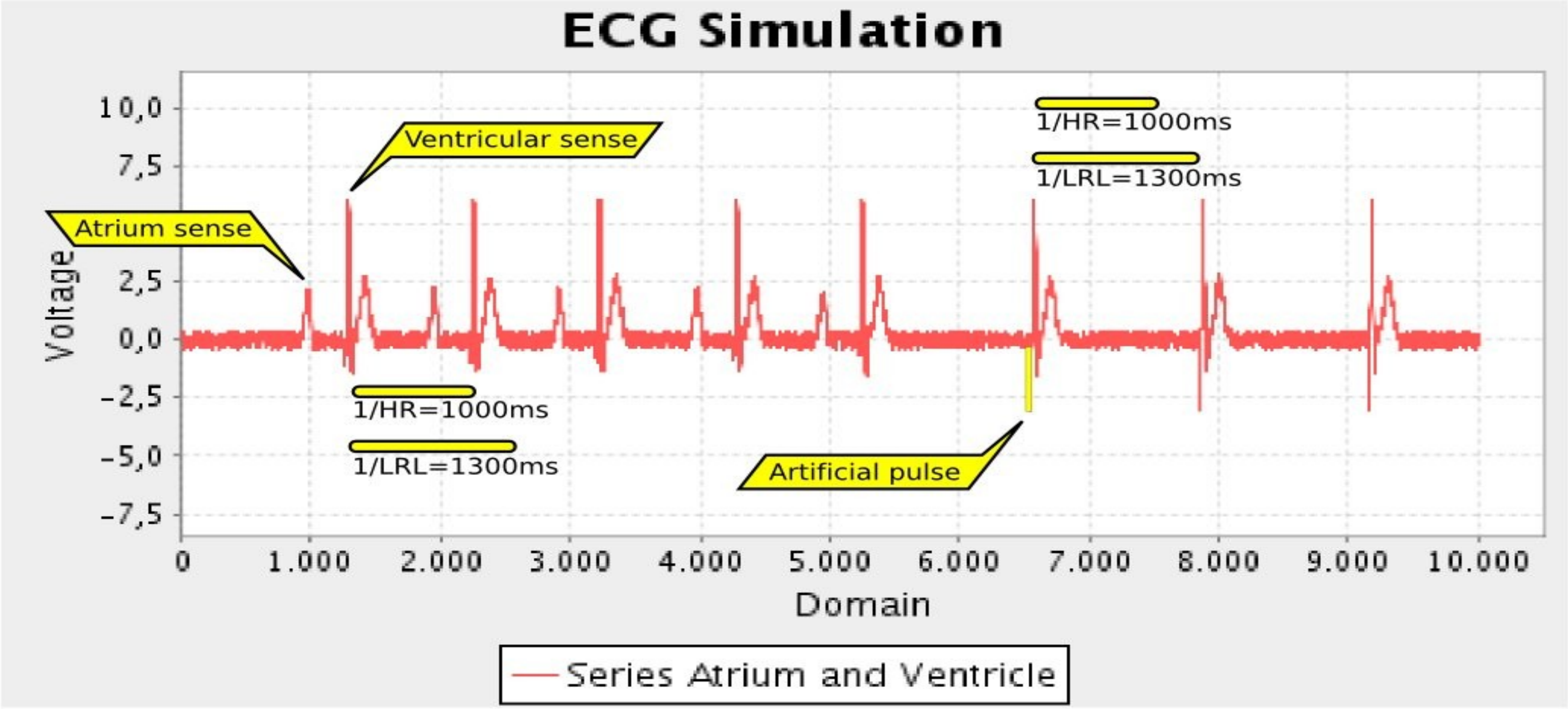
Java Simulator

- Heart parameters:
  - HAV(atrial-ventricular interval).
  - RR (natural heart period).
  - Wave Amplitudes.
  - Wave Durations.
- Pacemaker Parameters
  - Modes.
  - System Timeouts.
  - Refractory periods.



VVI Pacemaker Action

- At the beginning the heart has a natural pace which is regular and admissible.
- After a while the device is called to perform ventricular artificial pulses to resume the heart rate (HR) over the lower rate limit (LRL).



Conclusions

- The use of the TRIO language allowed us to produce a formal specification:
  - Readable and understandable.
  - Compact.
  - Supported by powerful tools.
- The approach proposed by the complementary use of ZOT and PVS guarantees:
  - A full understanding of the requirements.
  - A very fast implementation step.
- The simulation:
  - Reflects the behavior expected in the analysis step thanks to very usable graphs.