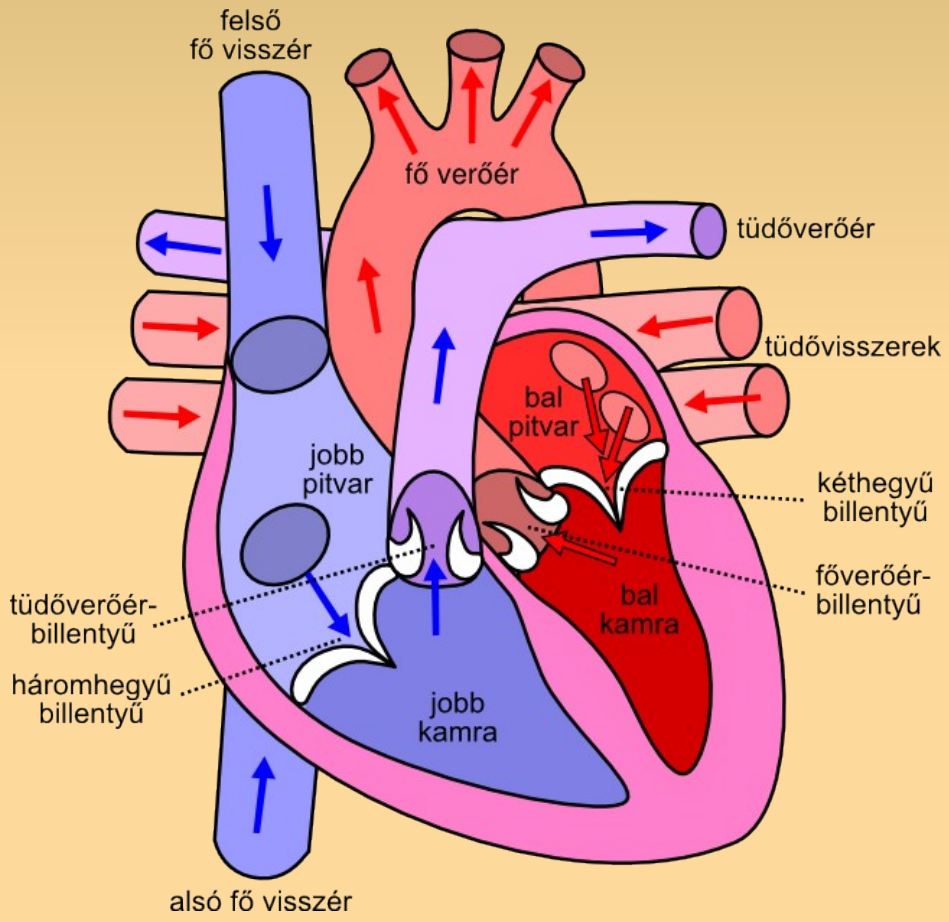
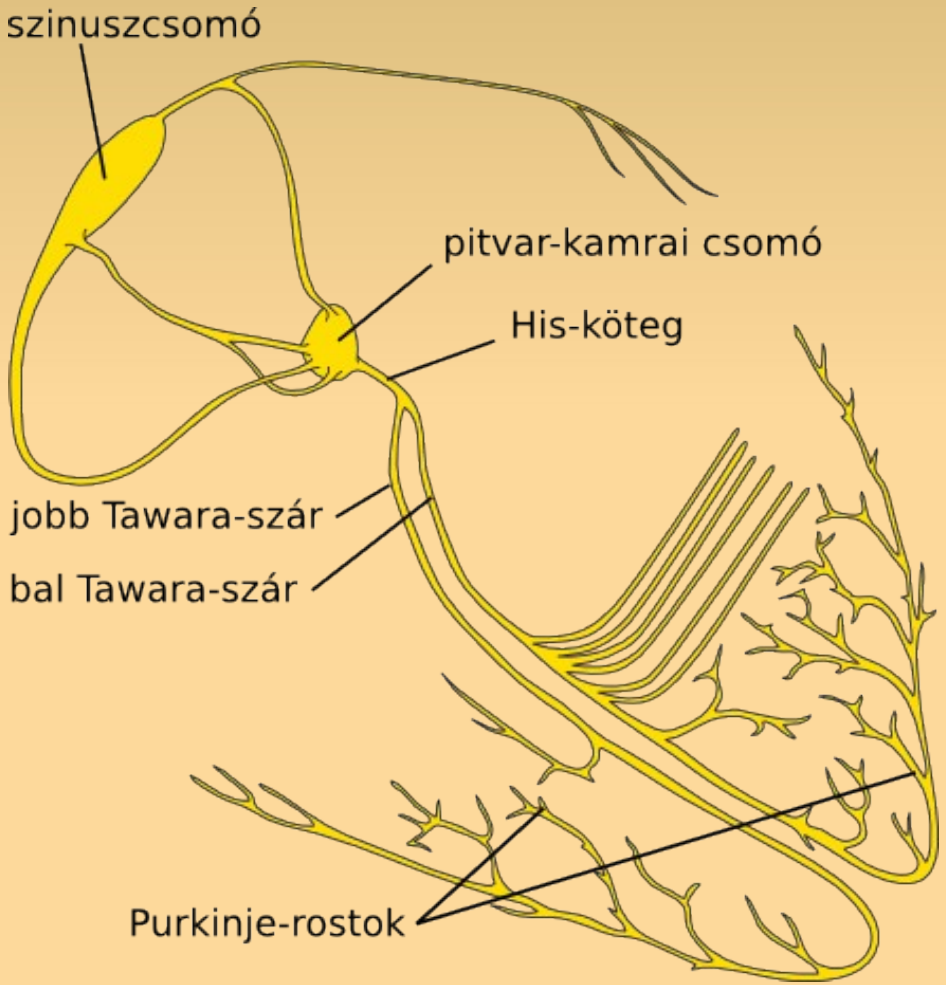
Pacemaker készülékek szoftverének verifikációja

Hesz Gábor

A szív felépítése





http://hu.wikipedia.org/w/index.php?title=Fájl:Diagram_of_the_human_heart_hu.svg

http://en.wikipedia.org/wiki/File:ConductionsystemoftheheartwithouttheHeart.png

Szívritmus-szabályozó

- implantátum
- szív elektromos aktivitásának monitorozása
- beavatkozás
  - elsődleges funkcionalitás: bradycardia elkerülése
  - másodlagos: tachycardia elkerülése, pitvar-kamra szinkron fenntartása, defibrilláció

Szabályozott kamrák	Érzékelt kamrák	Az érzékelésre adott válasz	Ritmus moduláció	Többhelyes ritmus-szabályozás
O = Nincs	O = Nincs	O = Nincs	O = Nincs	O = Nincs
A = Pitvar	A = Pitvar	T = Inger	R = Ritmus moduláció	A = Pitvar
V = Kamra	V = Kamra	I = Nincs inger		V = Kamra
D = Duális (A+V)	D = Duális (A+V)	D = Duális (T+I)		D = Duális (A+V)

Szívritmus-szabályozó felépítése

- **Érzékelő / beavatkozó elektródák**
  - A szívet és az eszközt kötik össze
  - uni- vagy bipoláris kapcsolat a szívfallal
- Pacemaker **generátor**
  - vezérlőegység és akkumulátor
- **Monitor** / programozó eszköz (DCM)
  - egy külső egység, amellyel az orvos kapcsolatba léphet a beépített egységgel (paraméterek beállítása, monitorozás, kézi vezérlés)
- Egyéb érzékelők:
  - Gyorsulásmérő, légzésfigyelő, véroxigénszint mérő, nyomásmérők, …

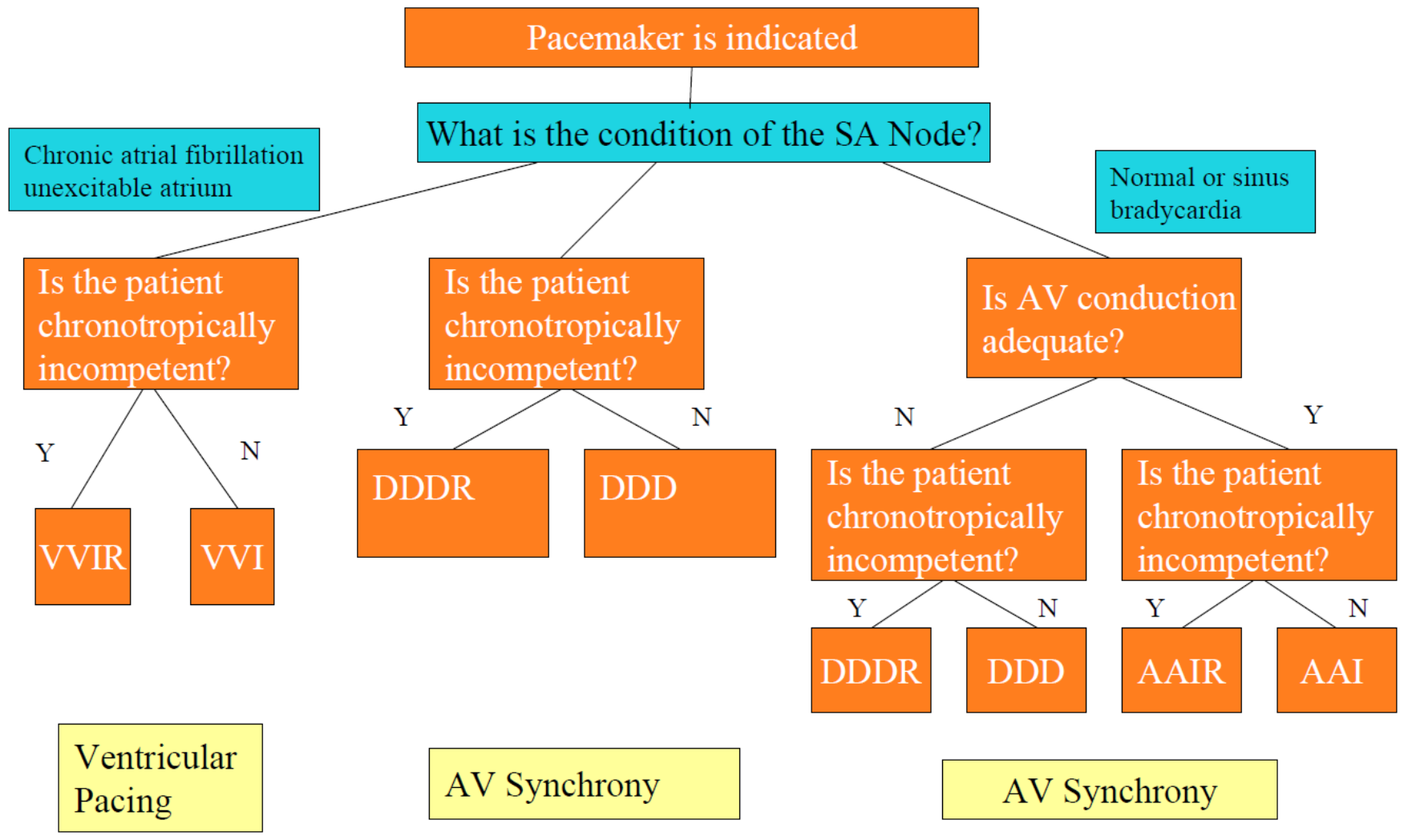
A kihívás

- (USA) 1990–2000 között több, mint 500 000 pacemakeres pácienst hívtak vissza meghibásodás miatt, az esetek 41%-a szoftver hiba
- Magyarországon kb 5500 beültetést végeznek évente
- Software Quality Research Laboratory (http://sqrl.mcmaster.ca/)
  - 2007, PACEMAKER Formal Methods Challenge
  - Korábbi generációs Boston Scientific pacemaker
  - Szívritmus-szabályozó informális specifikációja
  - Feladat: formális módszerekkel a szoftver leírása

Szívritmus-szabályozó paraméterei

Parameter	AAT	VVT	AOO	AAI	VOO	VVI	VDD	DOO	DDI	DDD	AOOR	AAIR	VOOR	VVIR	VDDR	DOOR	DDIR	DDDR
Lower Rate Limit	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Upper Rate Limit	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Maximum Sensor Rate											X	X	X	X	X	X	X	X
Fixed AV Delay							X	X	X	X					X	X	X	X
Dynamic AV Delay							X			X					X			X
Sensed AV Delay Offset										X								X
Atrial Amplitude	X		X	X				X	X	X	X	X				X	X	X
Ventricular Amplitude		X			X	X	X	X	X	X			X	X	X	X	X	X
Atrial Pulse Width	X		X	X				X	X	X	X	X				X	X	X
Ventricular Pulse Width		X			X	X	X	X	X	X			X	X	X	X	X	X
Atrial Sensitivity	X			X					X	X		X					X	X
Ventricular Sensitivity		X				X	X		X	X				X	X		X	X
VRP		X				X	X		X	X				X	X		X	X
ARP	X			X					X	X		X					X	X
PVARP	X			X					X	X		X					X	X
PVARP Extension							X			X					X			X
Hysteresis				X		X				X		X		X				X
Rate Smoothing				X		X	X			X		X		X	X			X
ATR Duration							X			X					X			X
ATR Fallback Mode							X			X					X			X
ATR Fallback Time							X			X					X			X
Activity Threshold											X	X	X	X	X	X	X	X
Reaction Time											X	X	X	X	X	X	X	X
Response Factor											X	X	X	X	X	X	X	X
Recovery Time											X	X	X	X	X	X	X	X

Optimális beavatkozás



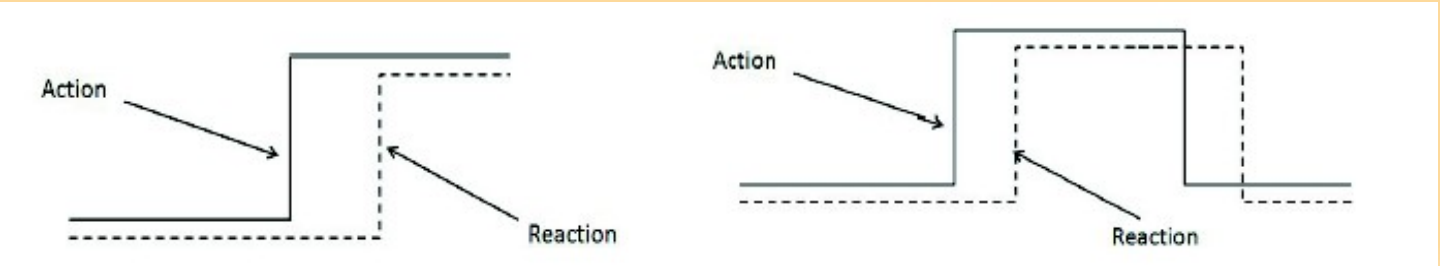
Szívritmus-szabályozó inkrementális fejlesztése

Dominique Méry, Neeraj Kumar Singh: Functional behavior of a cardiac pacing system, *International Journal of Discrete Event Control System*, Dec, 2010

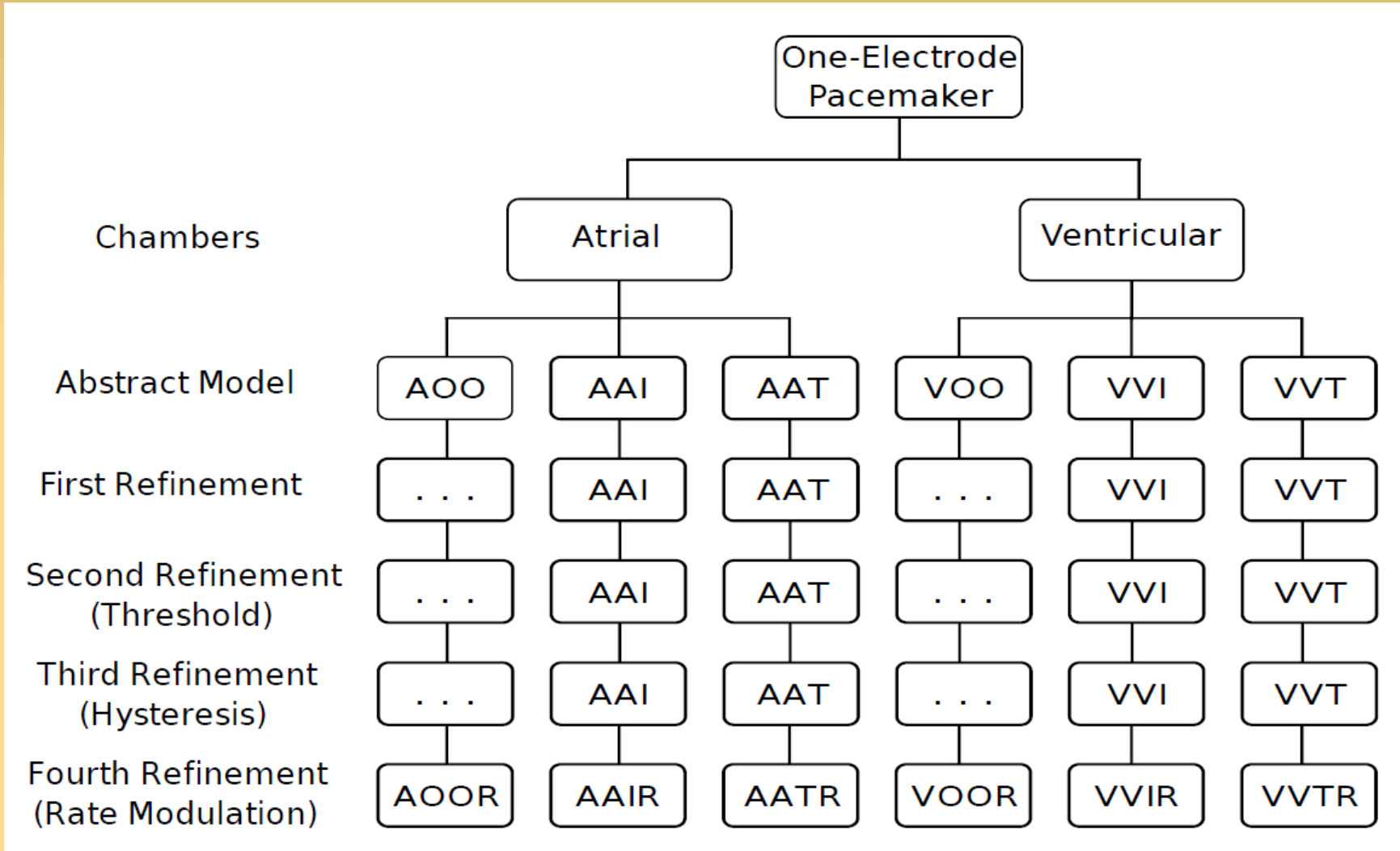
- INRIA / LORIA (Lorraine Research Laboratory in Computer Science and its Applications), Université Henri Poincaré, Nancy
- Event-B, absztrakt modell és finomítási lépések
- Eszközök:
  - RODIN – tervező IDE (Eclipse alapon)
  - ProB – tételbizonyító
  - EB2ALL – kódgenerátor (C, C#, Java, ...)

Tervezési minták

- Akció és gyenge reakció
  - Ha bekövetkezik egy akció, akkor egy reakcióval kell válaszolni rá.
  - A reakció nem követi pontosan az akciót, például ha az túl gyorsan ismétlődik vagy túl rövid ideig tart.
- Akció és erős reakció
  - Az akciók és reakciók teljesen szinkronizálva történnek.



Egy elektródás pacemaker finomítási lépéseinek vázlata



Axiómák

$$
\begin{aligned}
&axm1 : LRL \in 30 \mathinner{..} 175 \\
&axm2 : URL \in 50 \mathinner{..} 175 \\
&axm3 : URI \in \mathbb{N}_1 \ \wedge URI = 60000/URL \\
&axm4 : LRI \in \mathbb{N}_1 \ \wedge LRI = 60000/LRL \\
&axm5 : status = \{ON, OFF\} \\
&axm6 : LRL < URL \\
&axm7 : URI < LRI
\end{aligned}
$$

- *Lower-Rate-Limit* és *Upper-Rate-Limit*
  - Paraméterként adott [szívverés per perc]
- *LR-* és *UR Interval*
  - számított [ms]
- *Status*
  - Beavatkozás aktív / inaktív

Absztrakt szintaxis egy elektródás pacemaker

$$
\begin{array}{l}
inv1 : Pace\_Actu \in status \\
inv2 : Pace\_Int \in URI \,..\, LRI \\
inv3 : sp \in 1 \,..\, Pace\_Int \\
inv4 : last\_sp \in \mathbb{N} \\
inv5 : sp \leq LRI \\
inv6 : last\_sp \geq URI \ \wedge last\_sp \leq LRI \\
inv7 : sp < Pace\_Int \ \Rightarrow \ Pace\_Actu = OFF \\
\hline
thm1 : Pace\_Actu = ON \Rightarrow sp = Pace\_Int
\end{array}
$$

- *Pace_Actu*
  - Beavatkozó szerv állapota
- *Pace_Int:*
  - Beavatkozások intervalluma [ms]

- *Sp:* órajel, az utolsó beavatkozás óta eltelt idő
- *Last_sp:* a megelőző beavatkozások között eltelt idő
- *Inv5, Inv6*: biztonsági előírások a ritmus gyakoriságára
- *Inv7*: biztosítja, hogy a beavatkozó kikapcsolt állapotban van, két beavatkozás között
- *Thm1*: tétel, ha az beavatkozó működik, akkor *sp* = *Pace_Int*

Absztrakt események

- *Pace_ON*: tüzelés indítása, ha a beavatkozó kikapcsolt állapotban van és a számlálónk elérte a beállított intervallumot. Jegyezzük meg az utolsó intervallum hosszát is *last_sp*-ben.
- *Pace_OFF*: tüzelés vége, ha a beavatkozó bekapcsolt állapotban van és a számlálónk elérte a beállított intervallumot.
- *Tic*: belső óra, minden ezredmásodpercnél eggyel növeljük a számlálót

EVENT Pace_ON
WHEN
$grd1: \ Pace\_Actu = OFF$
$grd2: \ sp = Pace\_Int$
THEN
$act1: \ Pace\_Actu := ON$
$act2: \ last\_sp := sp$
END

EVENT Pace_OFF
WHEN
$grd1: \ Pace\_Actu = ON$
$grd2: \ sp = Pace\_Int$
THEN
$act1: \ Pace\_Actu := OFF$
$act2: \ sp := 1$
END

EVENT tic
WHEN
$grd1: \ sp < Pace\_Int$
THEN
$act1: \ sp := sp + 1$
END

AAI és VVI üzemmódok

$$axm1: \ RF \in 150 \mathinner{..} 500$$
$$inv1: \ Pace\_Sensor \in status$$
$$inv2: \ last\_ss \in \mathbb{N}$$
$$inv3: \ last\_ss \geq RF \wedge last\_ss \leq Pace\_Int$$

- *RF (Refactory Period)*
  - Az az idő, amely alatt a szív regenerálódik egy impulzus után (ilyenkor érzéketlen egy újabb impulzusra)
- *Pace_Sensor*
  - Érzékelő, amely a szív saját impulzusait jelzi
- *last_ss*
  - Az előző két érzékelés között eltelt idő

Események

EVENT Pace_OFF_with_Sensor
WHEN
$grd1: \ Pace\_Actu = OFF$
$grd2: \ Pace\_Sensor = ON$
$grd3: \ sp \geq RF$
THEN
$act1: \ last\_ss := sp$
$act2: \ sp := 1$
$act3: \ Pace\_Sensor := OFF$
END

EVENT Sense_ON
WHERE
grd1 : $Pacemaker\_Sensor = OFF$
grd2 : $sp \geq RF$
grd3 : $sp < Pace\_Int$
THEN
act1 : $Pacemaker\_Sensor := ON$
END

- *Pace_OFF_with_Sensor*
  - Újraindítja a számlálót, ha a szív saját szabályozása tüzel
- *Sense_ON*
  - Érzékelés akkor történhet, amikor a számlálónk *RF* és *Pace_Int* között van valahol.

Első finomítás

$$
\begin{aligned}
&inv1: \ sp < RF \Rightarrow Pace\_Sensor = OFF \\
&inv2: \ sp < RF \Rightarrow Pace\_Actu = OFF \\
&inv3: \ sp > RF \wedge sp \leq Pace\_Int \Rightarrow \\
&\qquad Pace\_Sensor = ON
\end{aligned}
$$

$$
\begin{aligned}
&grd1: \ (sp < RF \wedge Pace\_Sensor = OFF \wedge \\
&\qquad Pace\_Actu = OFF) \\
&\qquad \vee \\
&\qquad (sp \geq RF \wedge sp < Pace\_Int \wedge \\
&\qquad Pace\_Sensor = ON \wedge Pace\_Actu = OFF)
\end{aligned}
$$

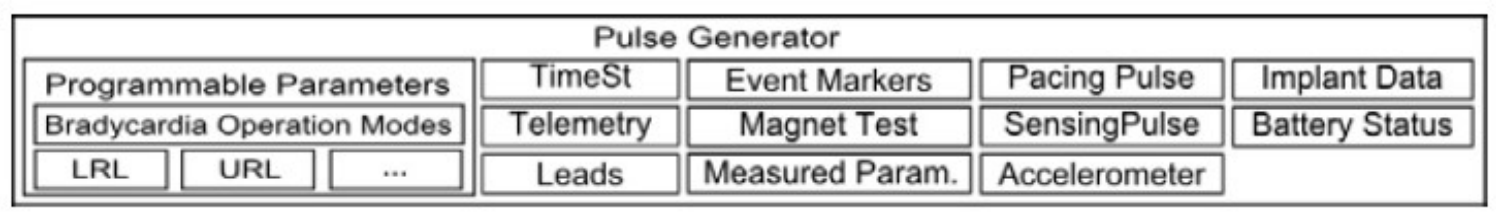
- Új invariánsok, amelyek biztosítják, hogy az RF periódus alatt az érzékelő és a beavatkozó szerv is inaktív
- A „*tic*” esemény feltételének finomítása

Bizonyítás

Model	Total number of POs	Automatic Proof	Interactive Proof
One-electrode pacemaker			
Abstract Model	118	114(96%)	4(4%)
First Refinement	60	44(73%)	16(27%)
Second Refinement	44	40(91%)	4(9%)
Third Refinement	36	24(66%)	12(34%)
Fourth Refinement	78	78(100%)	0(0%)
Two-electrode pacemaker			
Abstract Model	166	125(76%)	41(24%)
First Refinement	211	190(90%)	21(10%)
Second Refinement	67	66(99%)	1(1%)
Total	780	681(87%)	99(13%)

Formális pacemaker modell Z nyelven

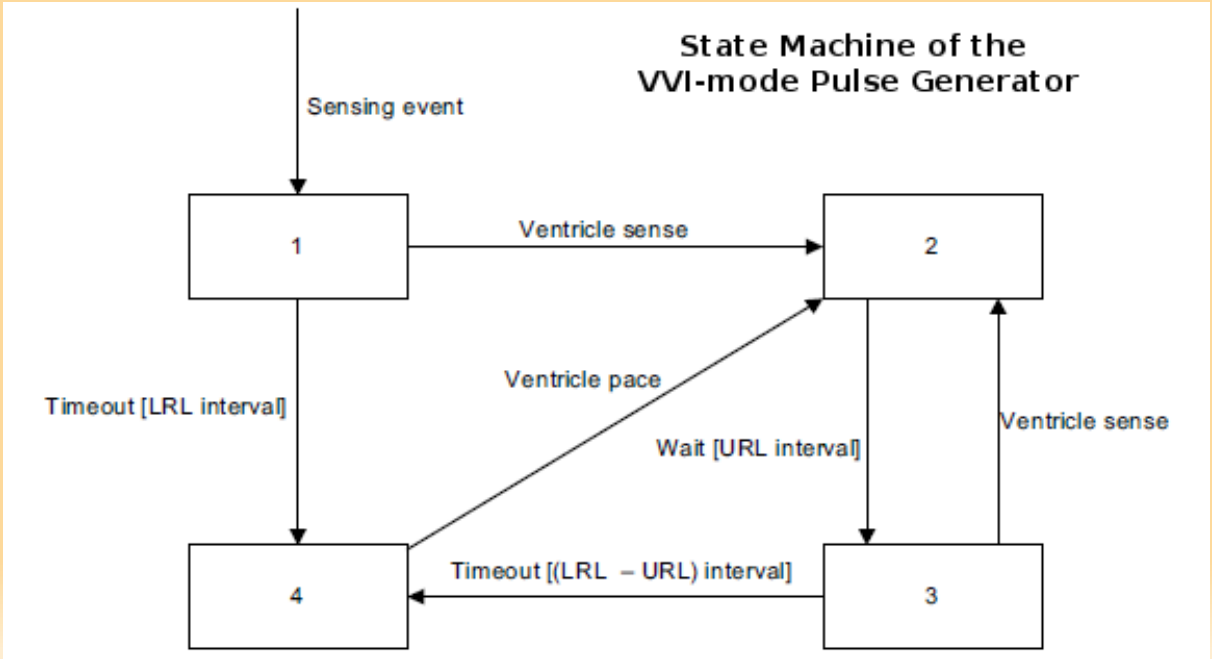
- A.O. Gomes és M.V.M. Oliveira
  - A. O. Gomes and M. V. M. Oliveira: Formal specification of a cardiac pacing system, in FM 2009, 2009, pp. 692–707.
  - Artur O. Gomes and Marcel V. M. Oliveira: Formal development of a cardiac pacemaker: from specification to code *Proceedings of the 13th Brazilian conference on Formal methods: foundations and applications,* 2011
- Z → Perfect Developer
  - 560 bizonyítandó állítás
  - 9000 soros verifikált C# programkód



Valósidejű pacemaker-modell

- Tuan, L.A., Zheng, M.C., Tho, Q.T.: Modeling and Verification of Safety Critical Systems: A Case Study on Pacemaker. *Fourth IEEE International Conference on Secure Software Integration and Reliability Improvement*. IEEE Press, Los Alamitos (2010)

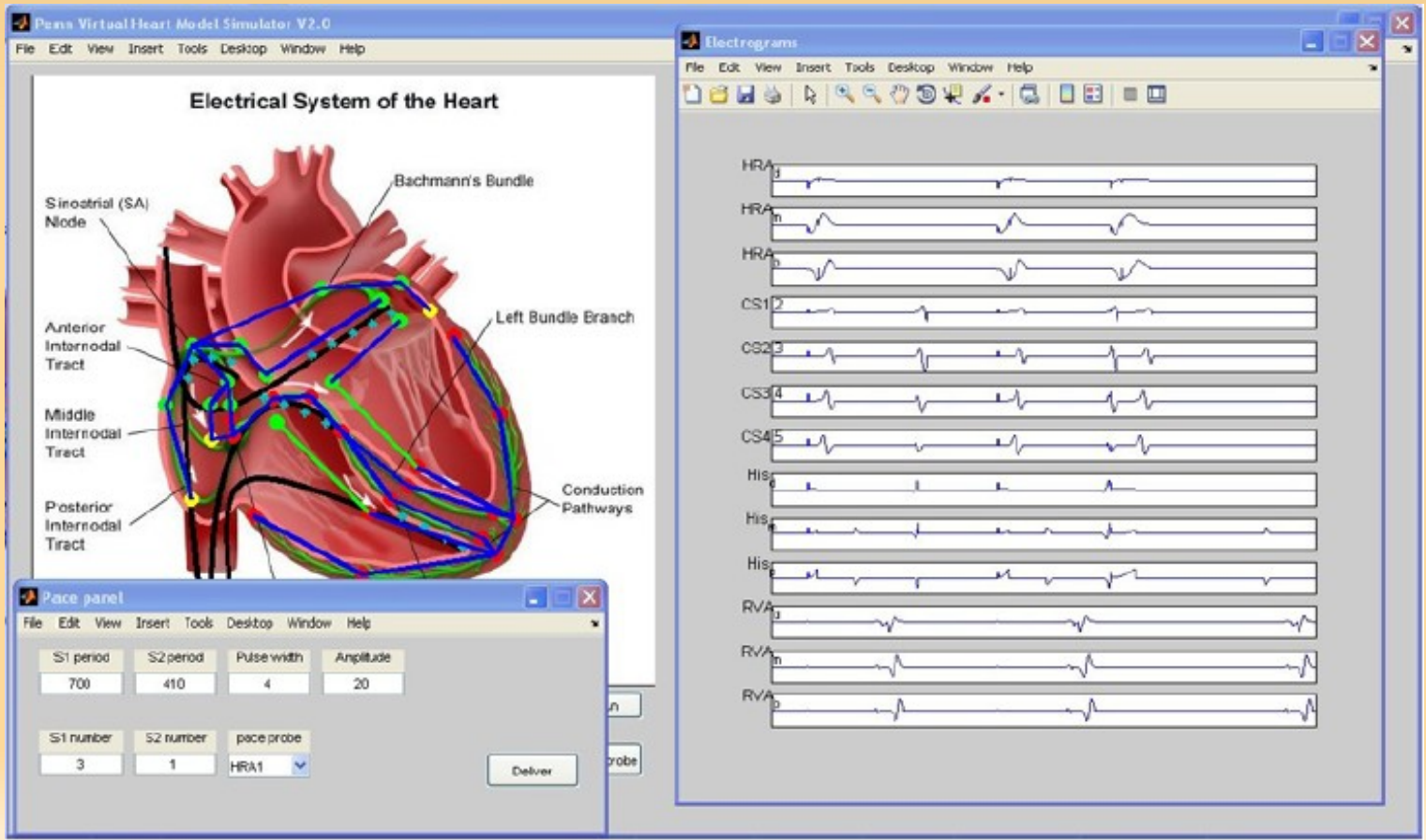
- Saját bizonyító eszköz (PAT)
  - P1 – Holtpont mentes
  - P2 – Minimum- és maximum pulzusszám
  - P3 – Regenerálódási idő
  - P4 – Pitvar–kamra késleltetés
  - P5 – Pulzus moduláció



Mode	P1	P2	P3	P4	P5
AAT	√	√	√	-	-
VVT	√	√	√	-	-
AOO	√	√	√	-	-
AAI	√	√	√	-	-
VOO	√	√	√	-	-
VVI	√	√	√	-	-
VDD	√	√	√	√	-
DOO	√	√	√	√	-
DDI	√	√	√	√	-
DDD	√	√	√	√	-
AOOR	√	√	√	-	√
AAIR	√	√	√	-	√
VOOR	√	√	√	-	√
VVIR	√	√	√	-	√
VDDR	√	√	√	√	√
DOOR	√	√	√	√	√
DDIR	√	√	√	√	√
DDDR	√	√	√	√	√

Validáció virtuális szívmodellel

- Zhihao Jiang, Allison Connolly és Rahul Mangharam (University of Pennsylvania)
  - Jiang Z, Connolly A, Mangharam R.: Using the Virtual Heart Model to validate the mode-switch pacemaker operation.
    Conf Proc IEEE Eng Med Biol Soc. 2010;2010:6690-3.
  - http://mlab.seas.upenn.edu/vhm



További kapcsolódó munkák

- H.D. Macedo et al.: elosztott valós idejű modell
  - H. D. Macedo, P. G. Larsen, and J. Fitzgerald,
    Incremental Development of a Distributed Real-Time Model of a Cardiac Pacing System Using VDM,
    ser. LNCS. Los Alamitos, CA, USA: Springer, 2008, pp. 181–197.
- V.P. Manna et al.: egyszerű szívritmus-szabályozó implementálása
  - V. P. L. Manna, A. T. Bonanno, and A. Motta,
    Poster on a simple pacemaker implementation.
    ACM, May 2009.

Köszönöm a figyelmet!

Irodalomjegyzék

- http://hu.wikipedia.org/wiki/Pacemaker
- http://en.wikipedia.org/wiki/Sinoatrial_node
- Software Quality Research Laboratory (http://sqrl.mcmaster.ca/, http://sqrl.mcmaster.ca/_SQRLDocuments/PACEMAKER.pdf)