

Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste
I Semestre 2023

Lecture: Examples

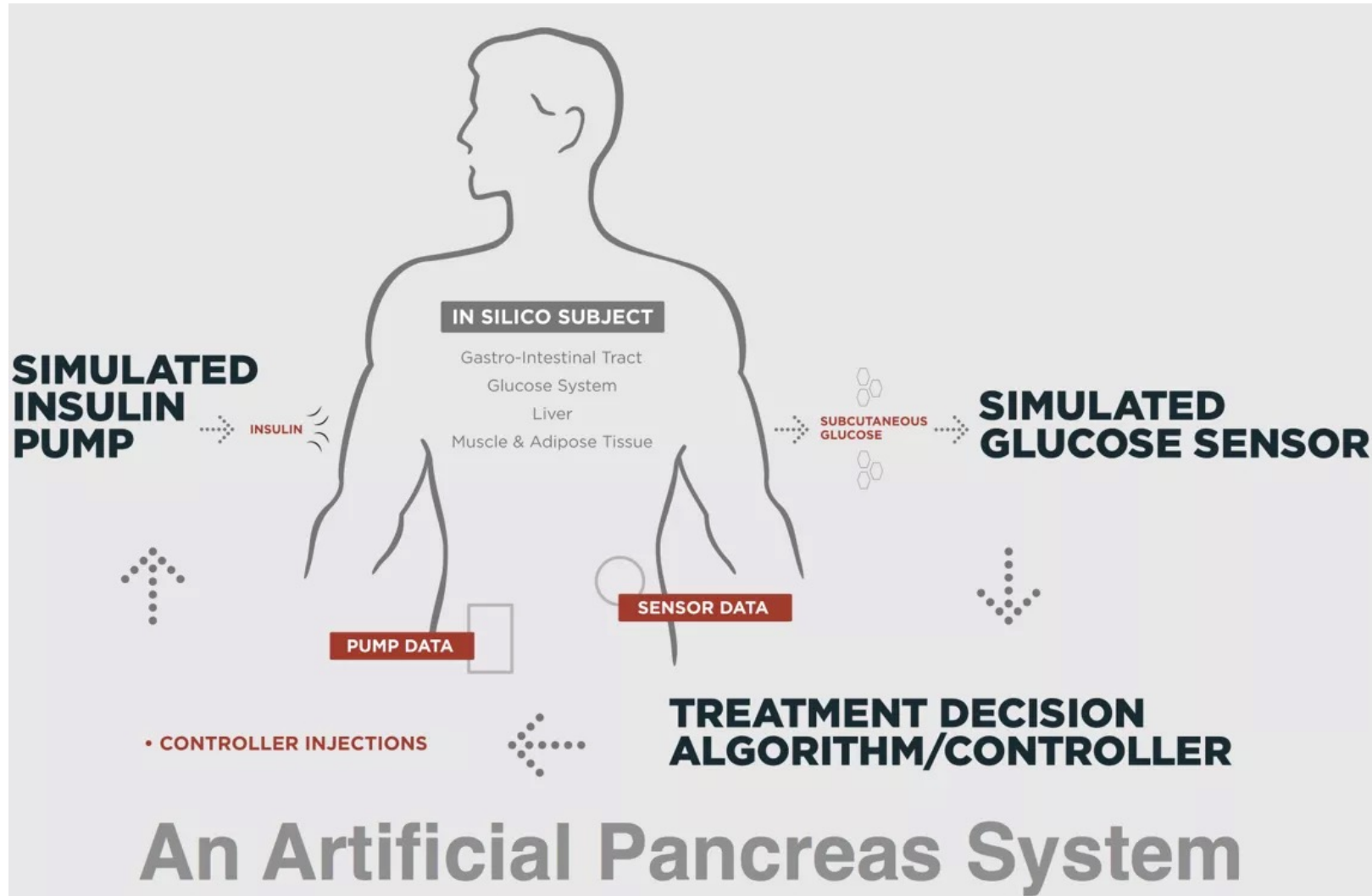
Artificial Pancreas

Type 1 diabetes occurs when the pancreas produces little or none of the insulin needed to regulate blood glucose

They rely on external administration of insulin to manage their blood glucose levels.



Artificial Pancreas



Stochastic Hybrid Systems Of Glucose

$$\frac{d}{dt} \mathbf{x}(t) = F(\mathbf{x}(t); u(t); \Theta);$$

$$y(t) = x_1(t)$$

glucose concentration

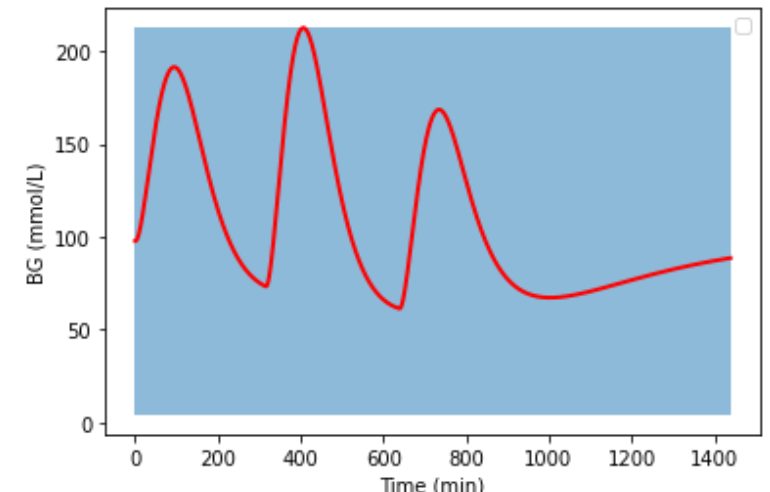
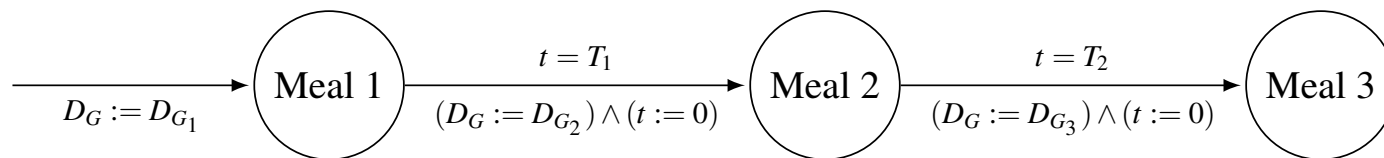
the control parameters

Infusion rate of bolus insulin

$\Theta = (D_{G_1}; D_{G_2}; D_{G_3}; T_1; T_2)$ are the control parameter

$(D_{G_1}; D_{G_2}; D_{G_3}) \in (N(40; 10); N(90; 10); N(60; 10))$ are the three daily meals

$(T_1; T_2) \in \sim N(300, 10)$ and $T_2 \sim N(300, 10)$ are the inter-times between each of them



Stochastic Hybrid Systems Of Glucose

$$\frac{d}{dt} Q_1(t) = -F_{01} - x_1 Q_1 + k_{12} Q_2 - F_R + EGP_0(1 - x_3) + \frac{D_G A_G}{t_{maxG}^2} t e^{-\frac{t}{t_{maxG}}}$$

$$\frac{d}{dt} Q_2(t) = x_1 Q_1 - (k_{12} + x_2) Q_2;$$

$$\frac{d}{dt} S_1(t) = u(t) + u_b - \frac{S_1}{t_{maxI}};$$

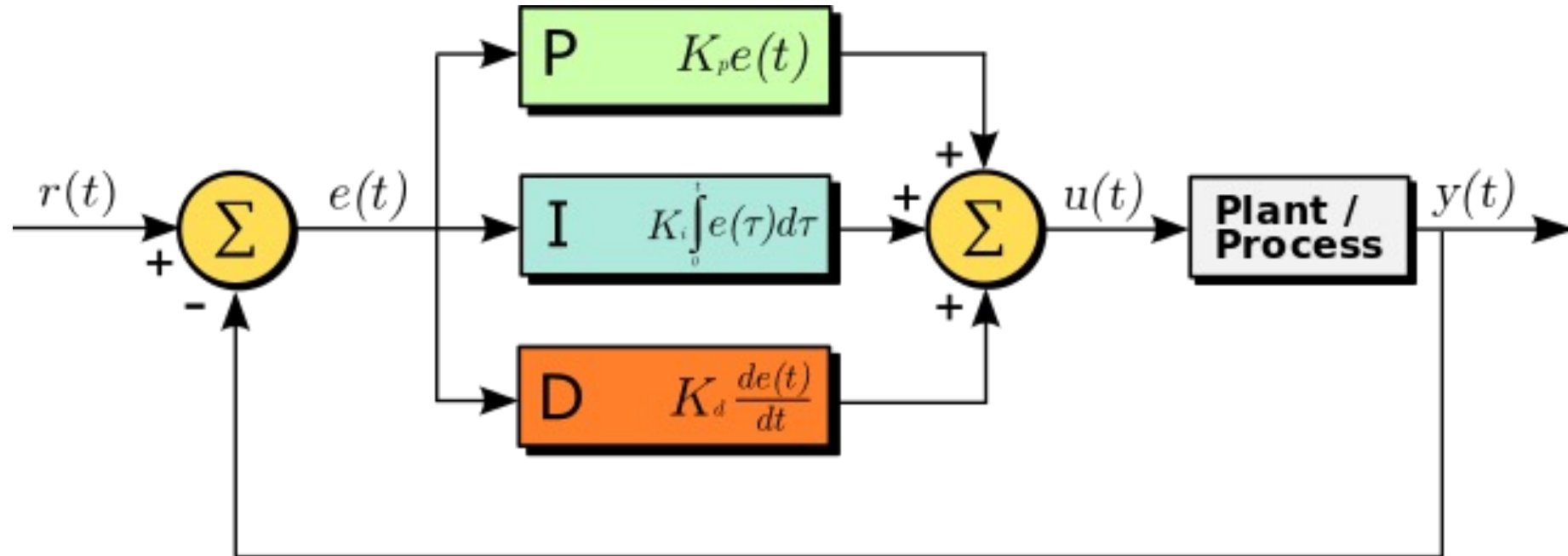
$$\frac{d}{dt} S_2(t) = S_1 - \frac{S_2}{t_{maxI}};$$

$$\frac{d}{dt} I(t) = \frac{S_2}{t_{maxI} V_I} - k_e I;$$

$$\frac{d}{dt} x_i(t) = -k_{a_i} x_i + k_{b_i} I; \quad (i = 1, 2, 3)$$

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau) d\tau + K_d \frac{d}{dt} e(t), \quad e(t) = r(t) - y(t)$$

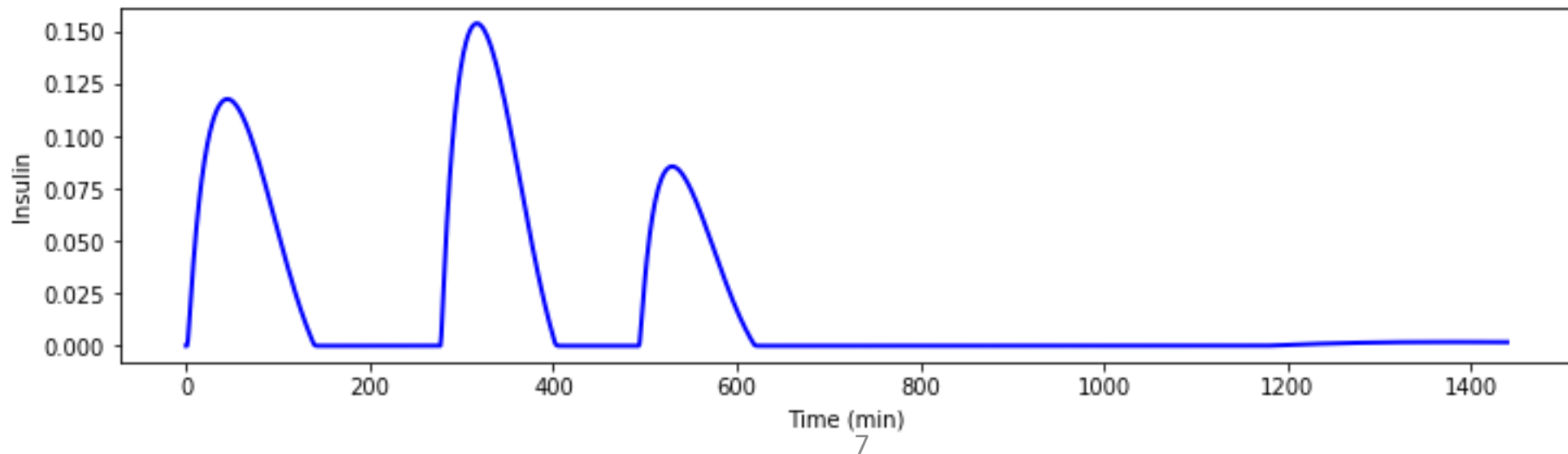
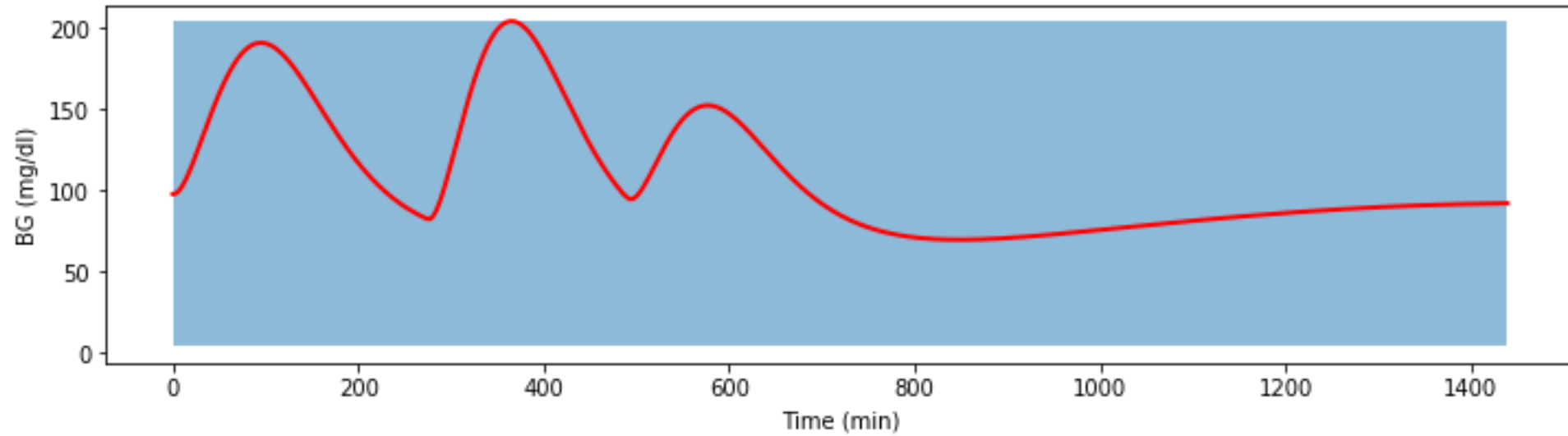
PID Control



$$u(t) = K_p e(t) + K_i \int_0^t e(\tau) d\tau + K_d \frac{d}{dt} e(t),$$

$$e(t) = r(t) - y(t)$$

Artificial Pancreas Simulation



STL Properties for the Artificial Pancreas

▶ Hyperglycemia

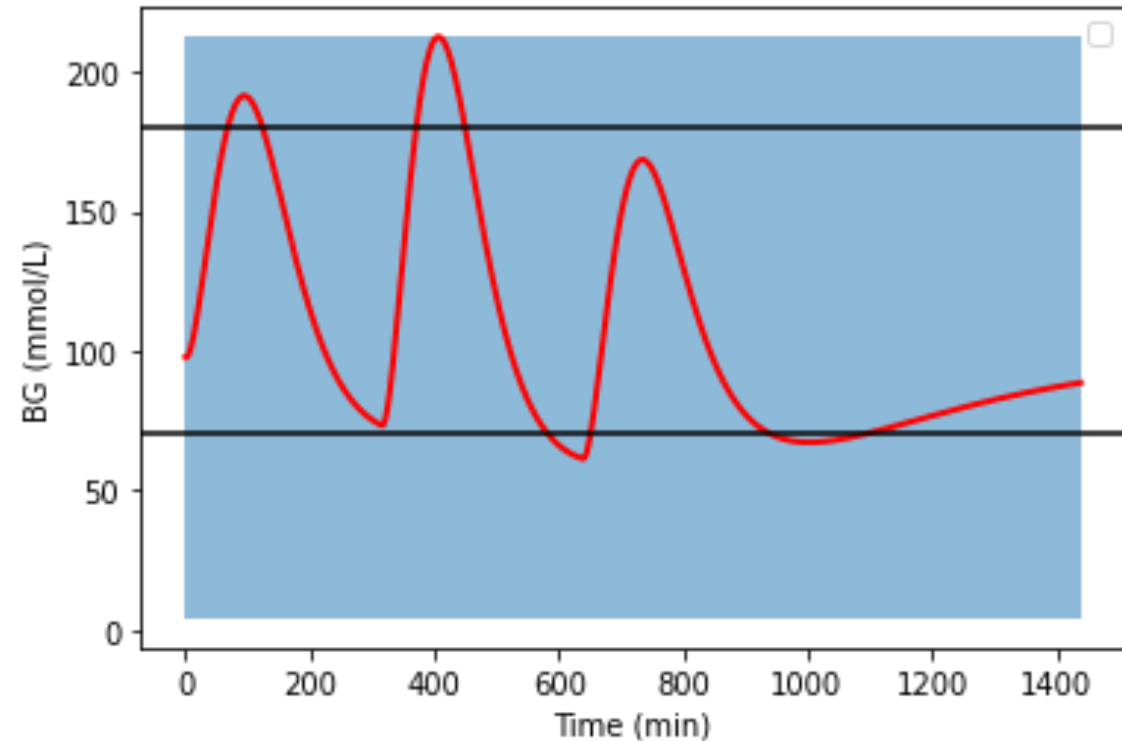
- ▶ “during the day the level of glucose goes above 180mg/dl”

$$\neg G_{[0,24h]}(BG(t) < 180)$$

▶ Hypoglycemia

- ▶ “during the day the level of glucose goes below 70mg/dl”

$$\neg G_{[0,24h]}(BG(t) > 70)$$



STL Properties for the Artificial Pancreas

▶ Prolonged Hyperglycemia

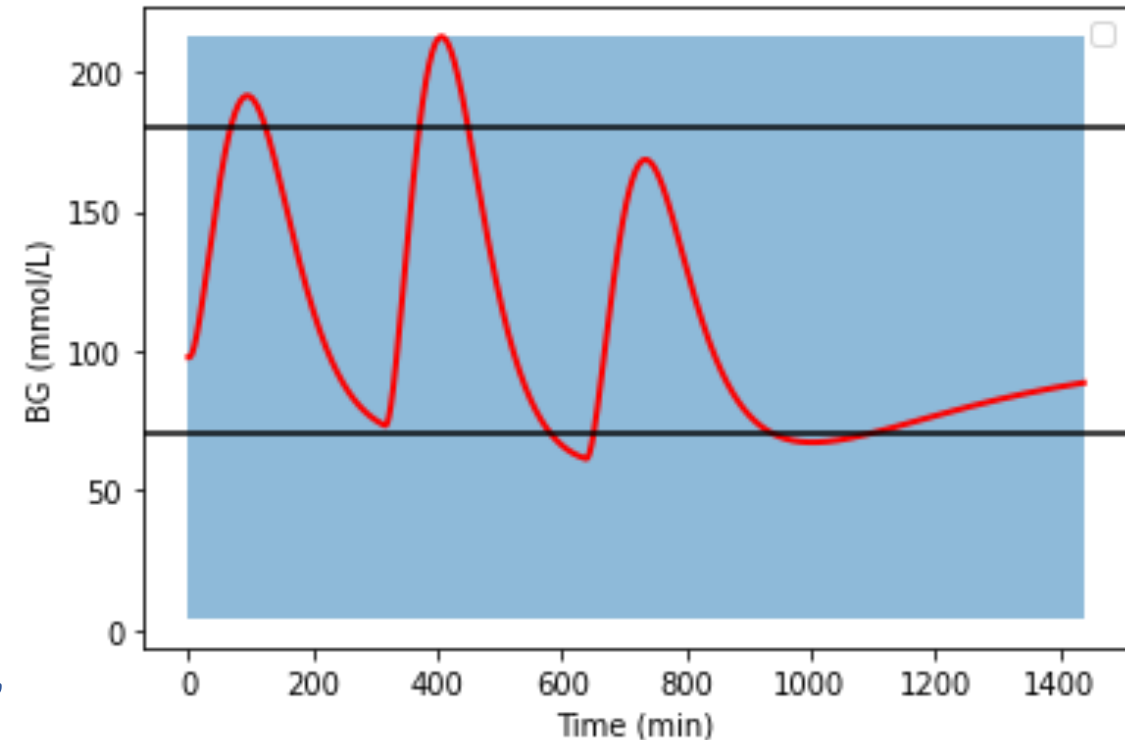
- ▶ “during the day the level of glucose goes above 180mg/dl for 3 hours”

$$F_{[0,21h]}(G_{[0,3]}(BG(t) \geq 180))$$

▶ Prolonged Hypoglycemia

- ▶ “during the day the level of glucose goes below 70mg/dl for 30 minutes”

$$F_{[0,21h]}(G_{[0,0.5]}(BG(t) < 70))$$



Falsification

The most simple way to do falsification with respect a property ϕ is minimizing the robustness over N iterations considering random samples on control parameters, i.e:

minSTL = 'inf'

For $i = 1, \dots, N$:

$\Theta = \text{sampling}(D_{G_1}, D_{G_2}, D_{G_3}, T_1, T_2)$

$t, y = \text{simulation}(\Theta)$

$\text{stl} = \text{computeRobustness}(y, \phi)$

if ($\text{stl} < \text{minSTL}$):

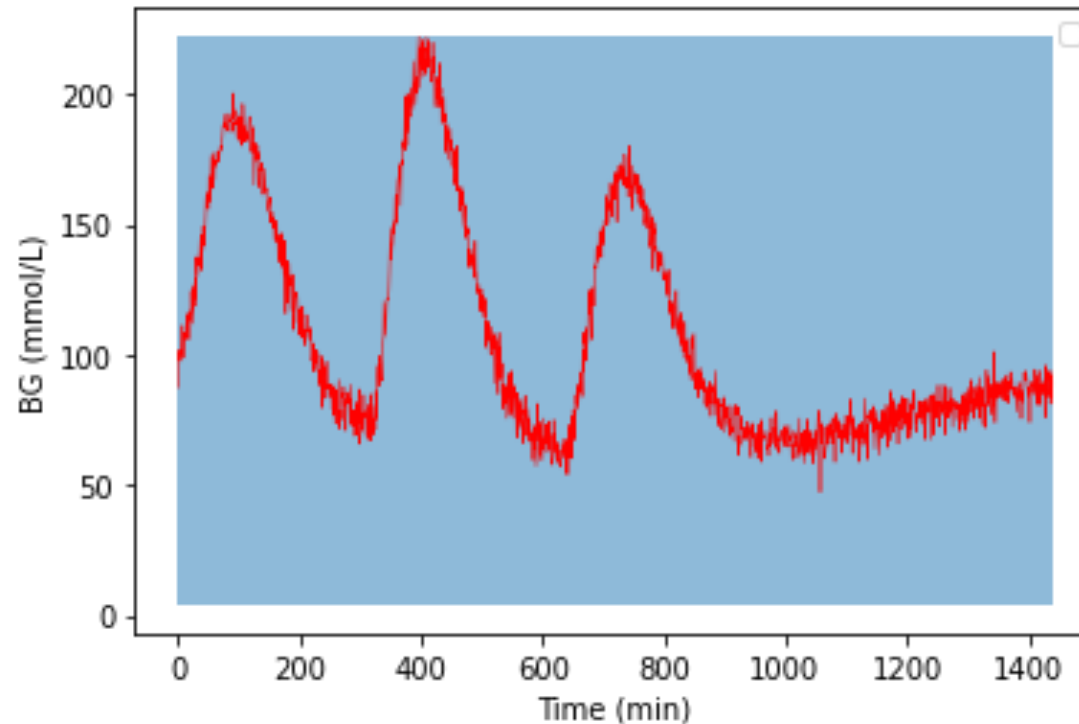
$\text{minSTL} = \text{stl}$

$\text{vSTL} = [D_{G_1}, D_{G_2}, D_{G_3}, T_1, T_2]$

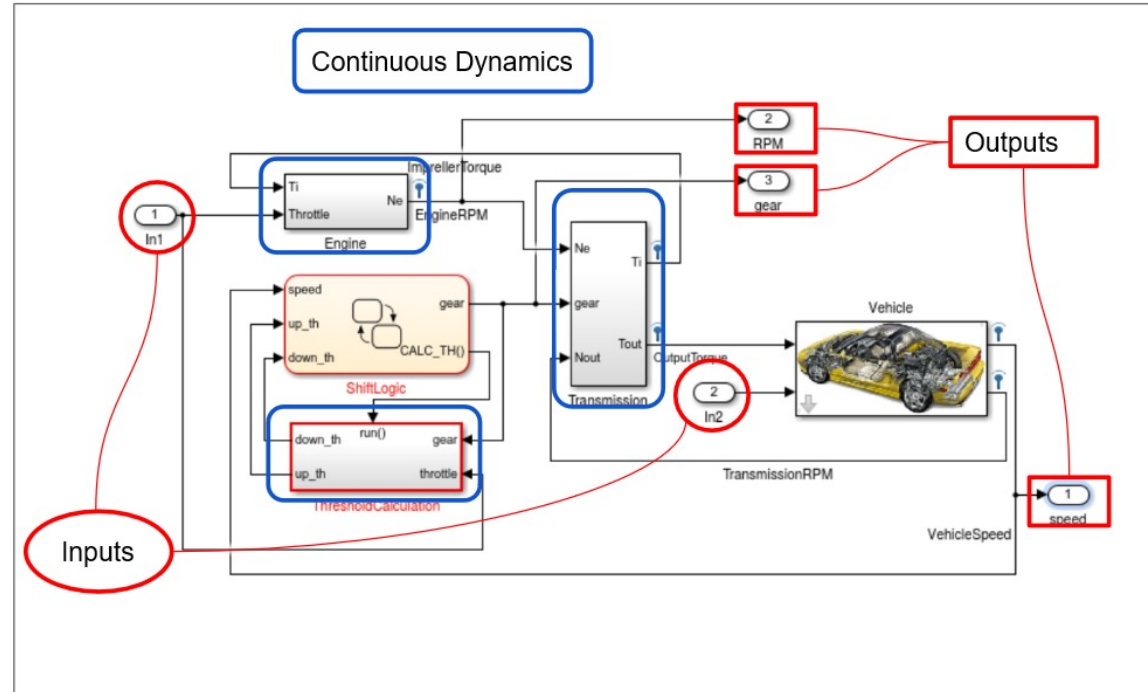
For fixed control parameter spaces you can consider to sample with respect to the grids over it.

Noise Robustness

- ▶ To consider noisy sensor we can add a Gaussian noise to the generated glucose trajectory, i.e. $GB(t) + \gamma$ with $\gamma \in N(0; 5)$



Automatic Transmission

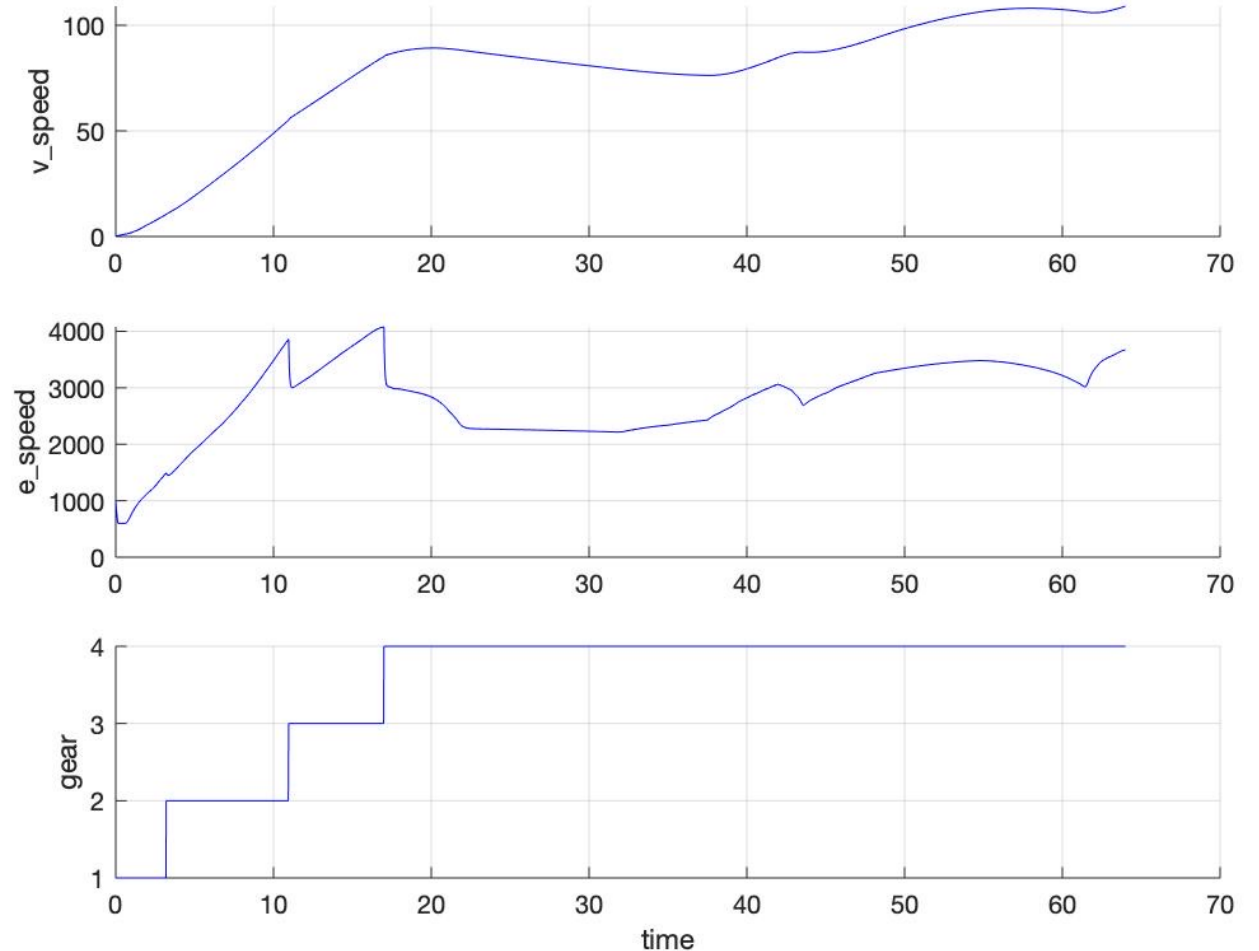


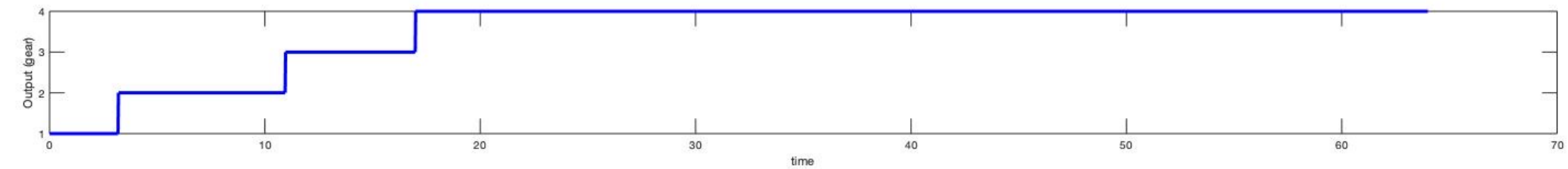
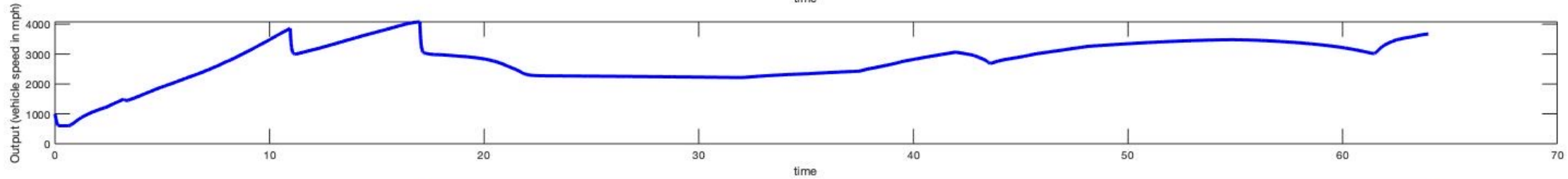
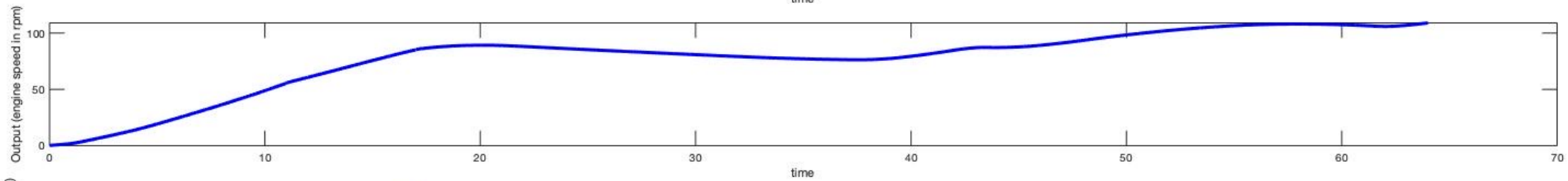
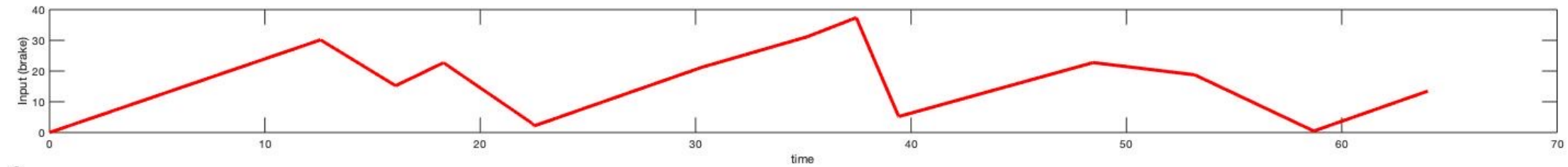
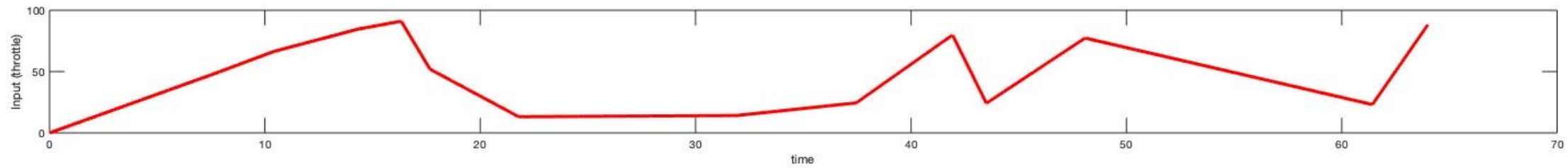
Most material that follows is from this paper:

- ▶ Bardh Hoxha, Houssam Abbas, Georgios E. Fainekos: Benchmarks for Temporal Logic Requirements for Automotive Systems. ARCH@CPSWeek 2014: 25-30

Automatic Transmission

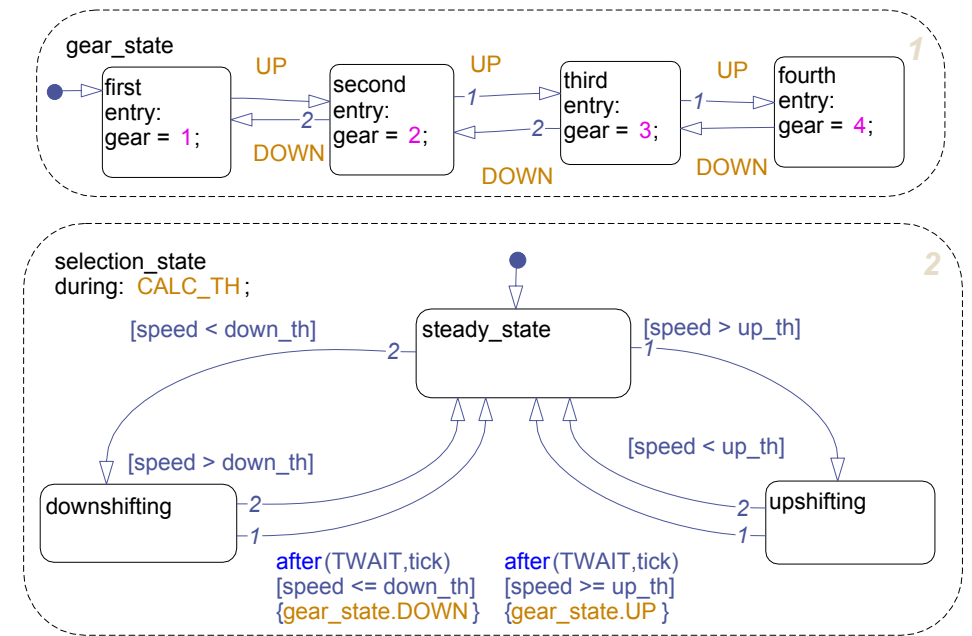
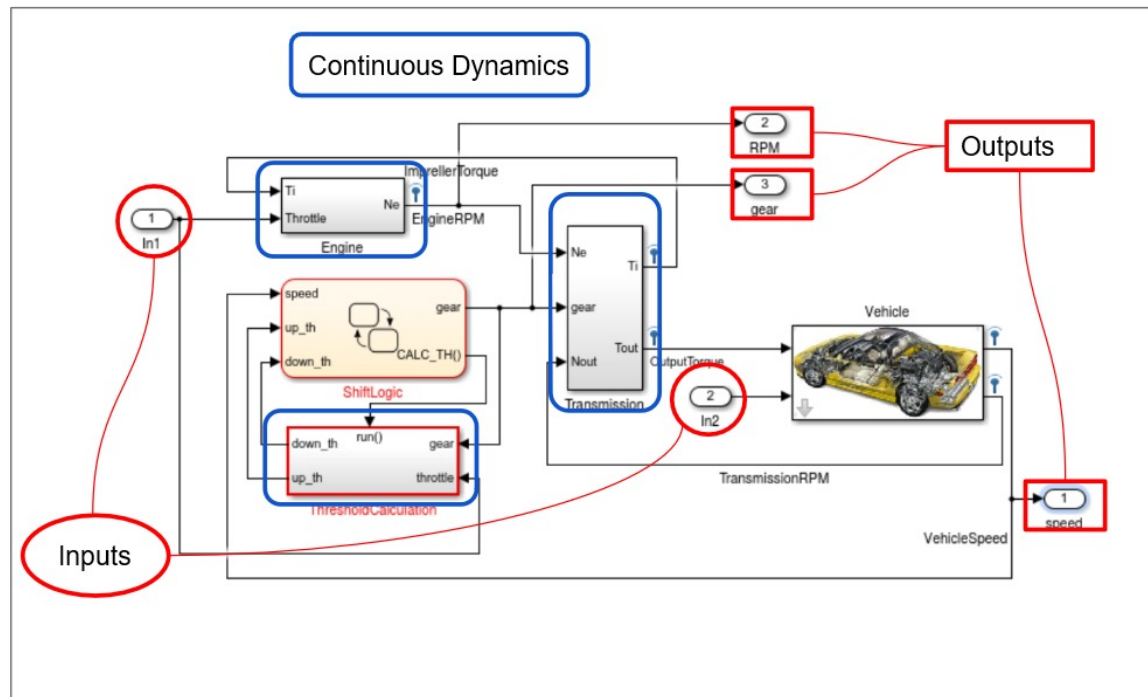
- ▶ Inputs: the throttle and break
- ▶ Outputs: the speed of the engine ω (RPM), the speed of the vehicle v (mph) and the gear.
- ▶ Initially, the vehicle is at rest at time 0, i.e. the speed $v = 0$ and engine speed $\omega = 0$
- ▶ Therefore, the output trajectories depend only on the input signals u_t and u_b which model the throttle and break inputs.
- ▶ The throttle and break, at each point in time, can take any value between 0 (fully closed) to 100 (fully open).





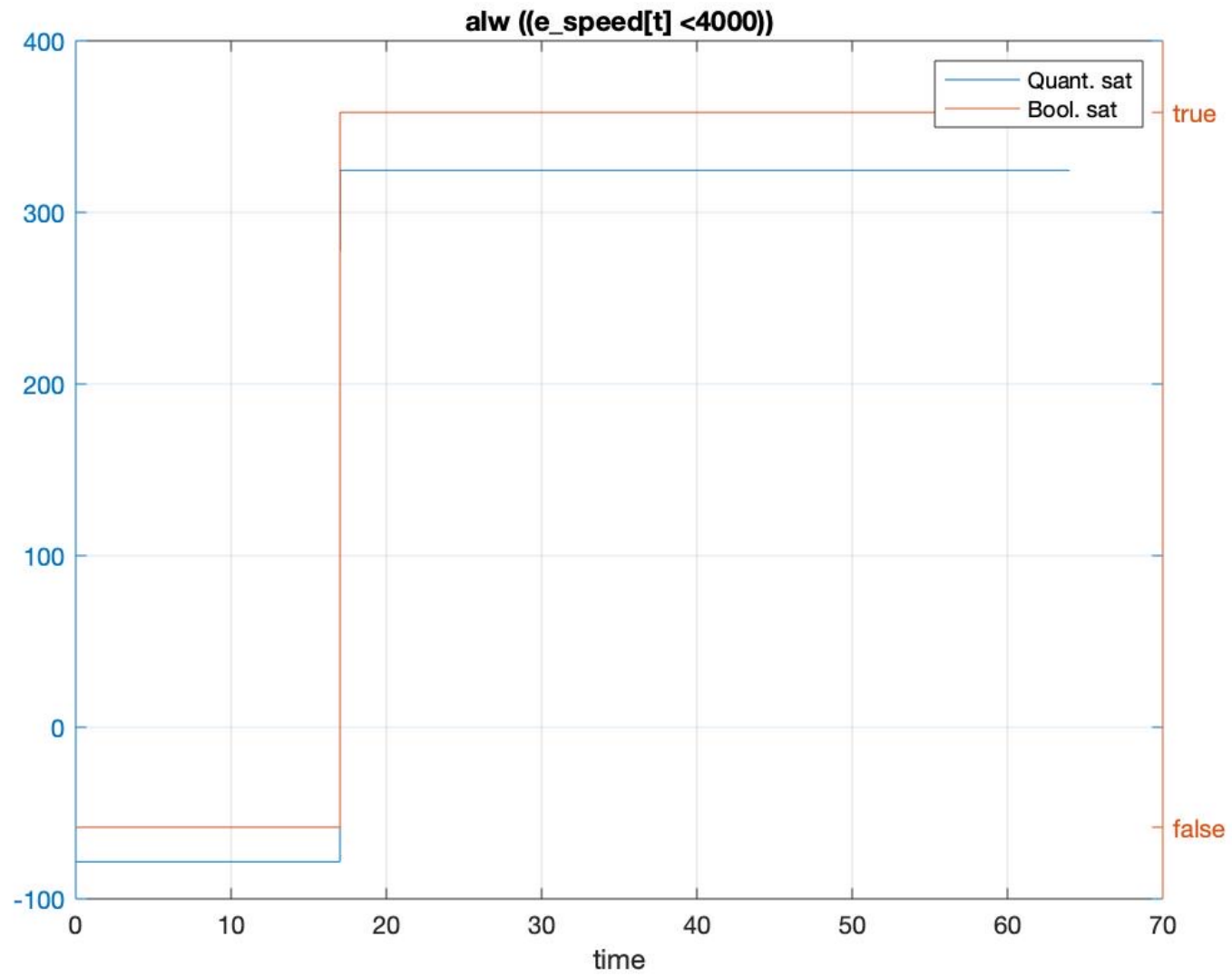
Automatic Transmission

- ▶ The model contains 69 blocks among which there are 2 integrators (i.e., 2 continuous state variables), and a Stateflow chart. The Stateflow chart contains two concurrently executing Finite State Machines with 4 and 3 states, respectively.

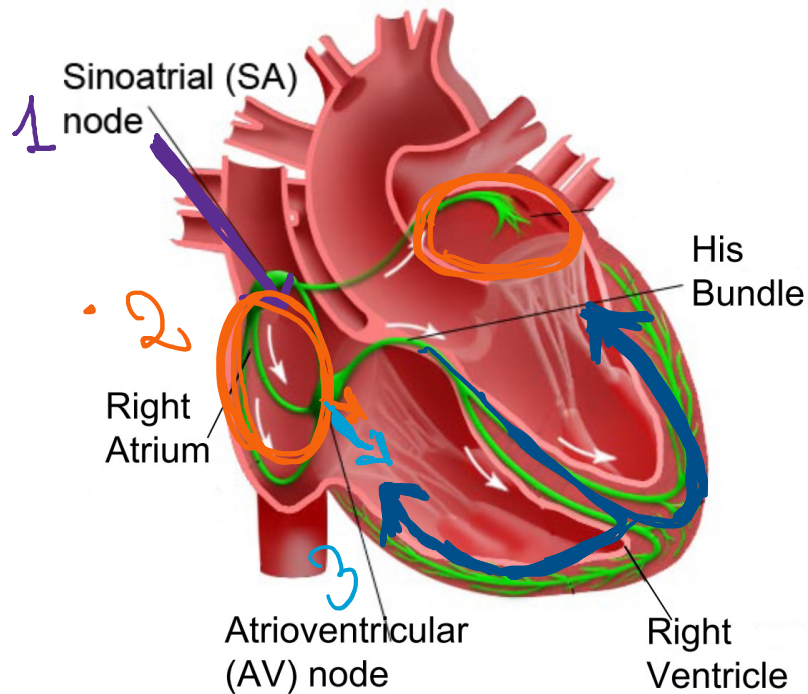


Properties

Automatic Transmission		
	Natural Language	MTL
ϕ_1^{AT}	The engine speed never reaches $\bar{\omega}$.	$\Box(\omega < \bar{\omega})$
ϕ_2^{AT}	The engine and the vehicle speed never reach $\bar{\omega}$ and \bar{v} , resp.	$\Box((\omega < \bar{\omega}) \wedge (v < \bar{v}))$
ϕ_3^{AT}	There should be no transition from gear two to gear one and back to gear two in less than 2.5 sec.	$\Box((g_2 \wedge Xg_1) \rightarrow \Box_{(0,2.5]}\neg g_2)$
ϕ_4^{AT}	After shifting into gear one, there should be no shift from gear one to any other gear within 2.5 sec.	$\Box((\neg g_1 \wedge Xg_1) \rightarrow \Box_{(0,2.5]}g_1)$
ϕ_5^{AT}	When shifting into any gear, there should be no shift from that gear to any other gear within 2.5sec.	$\bigwedge_{i=1}^4 \Box((\neg g_i \wedge Xg_i) \rightarrow \Box_{(0,2.5]}g_i)$
ϕ_6^{AT}	If engine speed is always less than $\bar{\omega}$, then vehicle speed can not exceed \bar{v} in less than T sec.	$\neg(\Diamond_{[0,T]}(v > \bar{v}) \wedge \Box(\omega < \bar{\omega}))$
ϕ_7^{AT}	Within T sec the vehicle speed is above \bar{v} and from that point on the engine speed is always less than $\bar{\omega}$.	$\Diamond_{[0,T]}((v \geq \bar{v}) \wedge \Box(\omega < \bar{\omega}))$
ϕ_8^{AT}	A gear increase from first to fourth in under 10secs, ending in an RPM above $\bar{\omega}$ within 2 seconds of that, should result in a vehicle speed above \bar{v} .	$((g_1 \mathcal{U} g_2 \mathcal{U} g_3 \mathcal{U} g_4) \wedge \Diamond_{[0,10]}(g_4 \wedge \Diamond_{[0,2]}(\omega \geq \bar{\omega}))) \rightarrow \Diamond_{[0,10]}(g_4 \rightarrow X(g_4 \mathcal{U}_{[0,1]}(v \geq \bar{v})))$



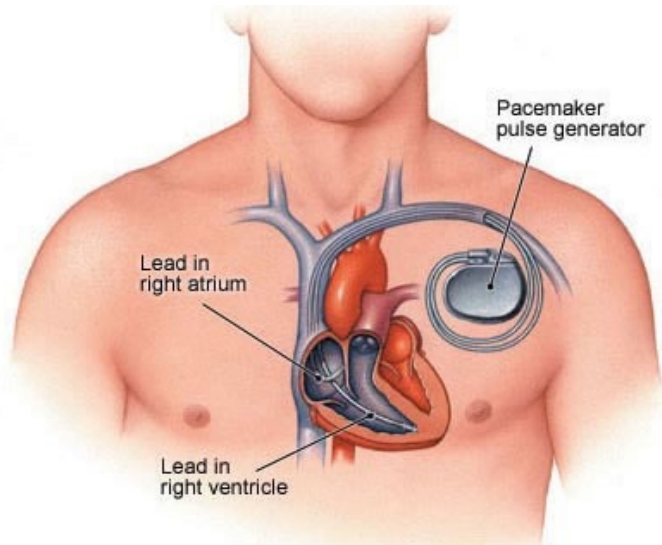
Pacemaker



- 1 ▶ SA node (controlled by nervous system) periodically generates an electric pulse
- 2 ▶ This pulse causes both atria to contract pushing blood into the ventricles
- 3 ▶ Conduction is delayed at the AV node allowing ventricles to full fill
- 4 ▶ Finally the His-Purkinje system spreads electric activation through ventricles causing them both to contract, pumping blood out of the heart

Electrical Conduction System of the Heart

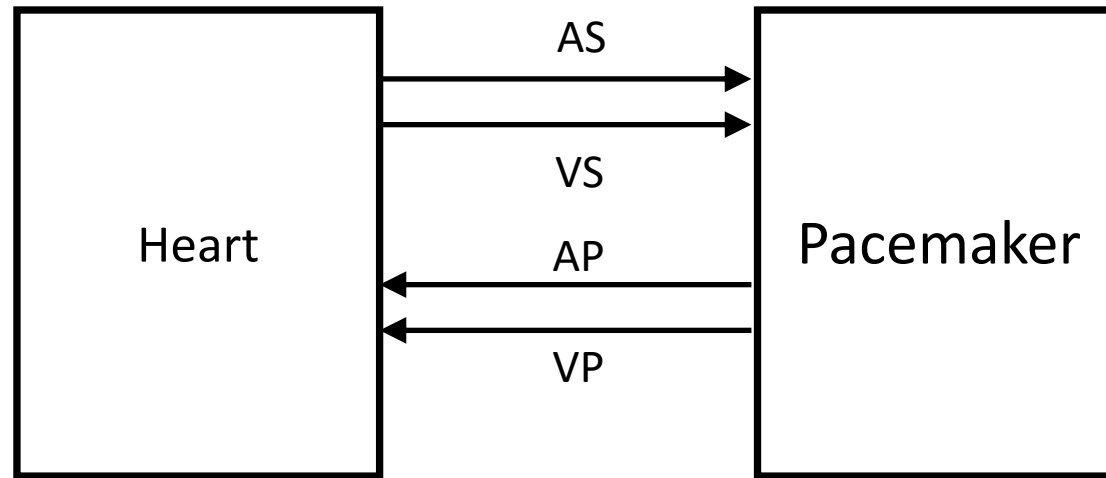
What do pacemakers do?



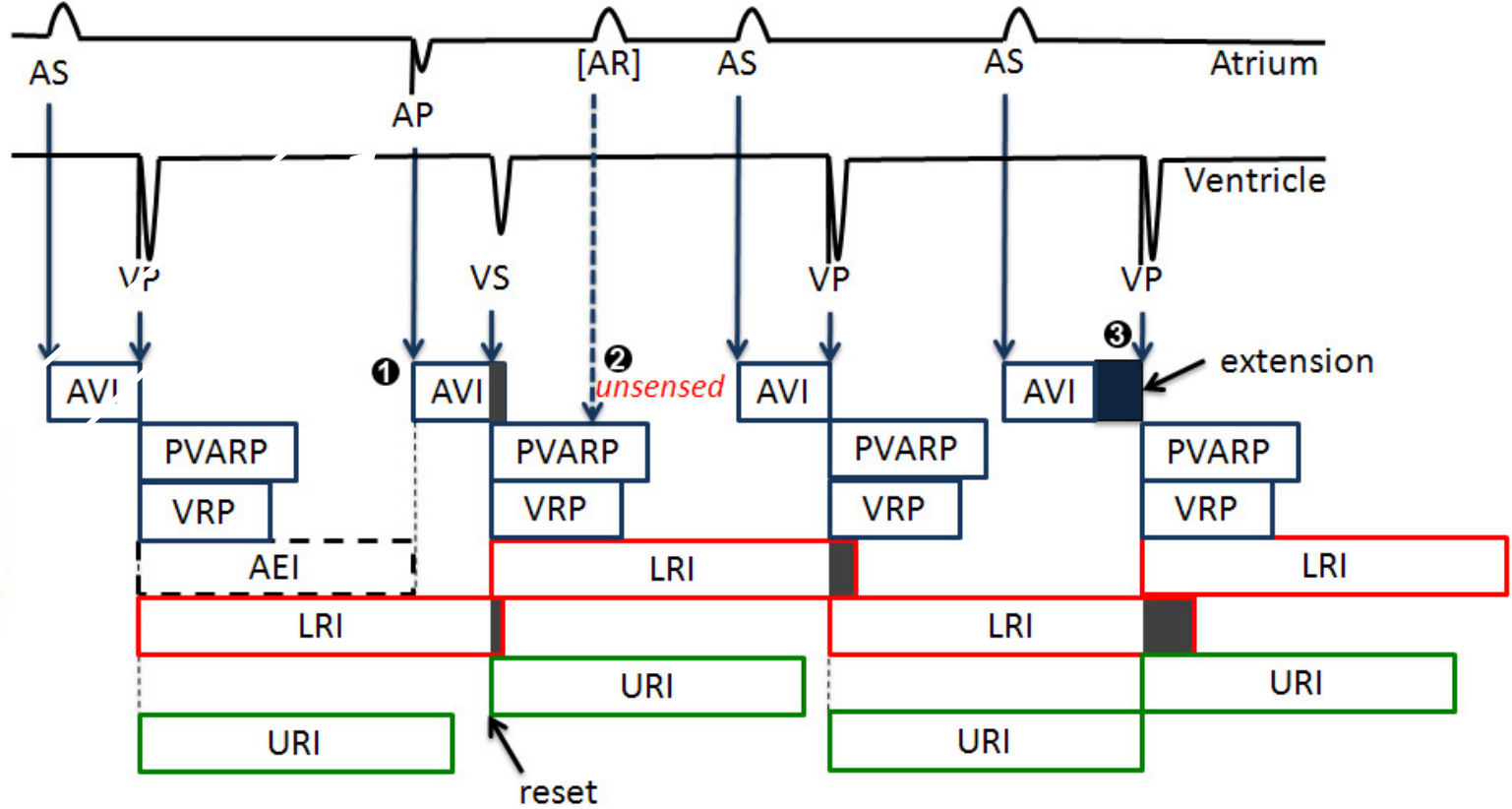
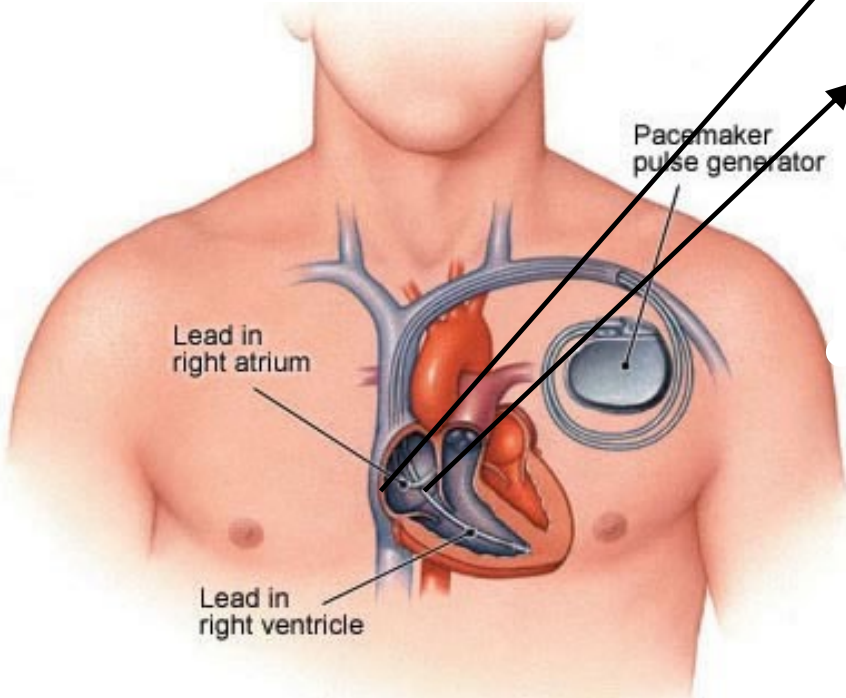
- ▶ Aging and/or diseases cause conduction properties of heart tissue to change leading to timing anomalies in heart rhythm (arrhythmias)
- ▶ Tachycardia: faster than desirable heart rate impairing hemo-dynamics (blood flow dynamics)
- ▶ Bradycardia: slower heart rate leading to insufficient blood supply
- ▶ Pacemakers can be used to treat bradycardia by providing pulses when heart rate is low

How dual-chamber pacemakers work

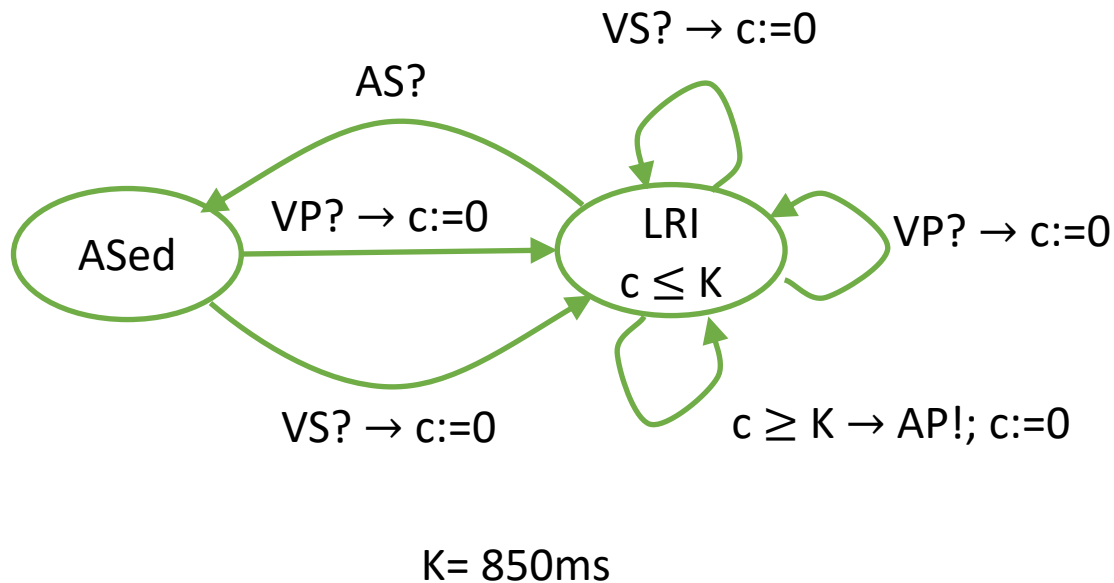
- ▶ Two fixed leads on wall of right atrium and ventricle respectively
- ▶ Activation of local tissue sensed by the leads (giving rise to events Atrial Sense (AS) and Ventricular Sense (VS))
- ▶ Atrial Pacing (AP) or Ventricular Pacing (VP) are delivered if no sensed events occur within deadlines



Implantable Pacemaker modeling

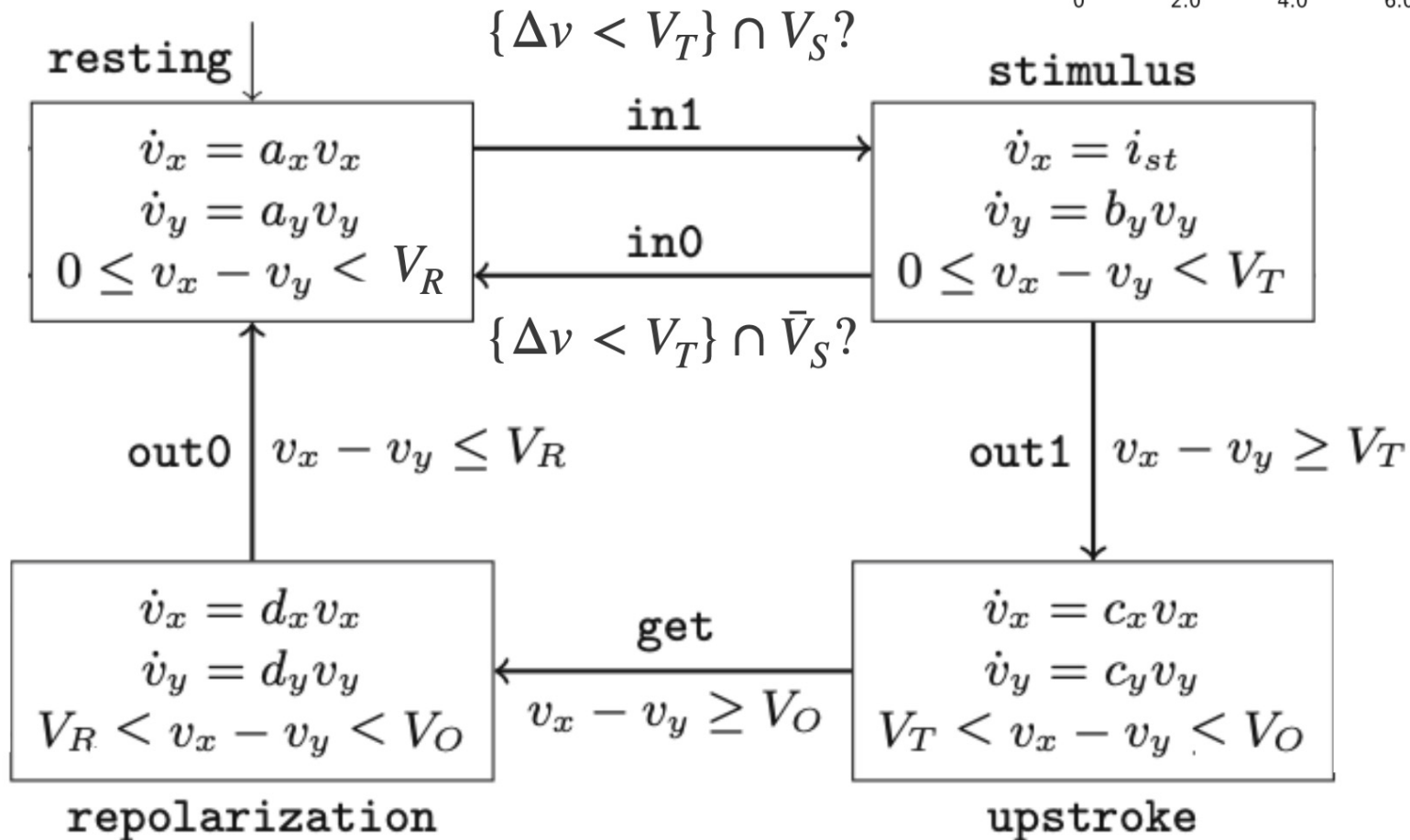
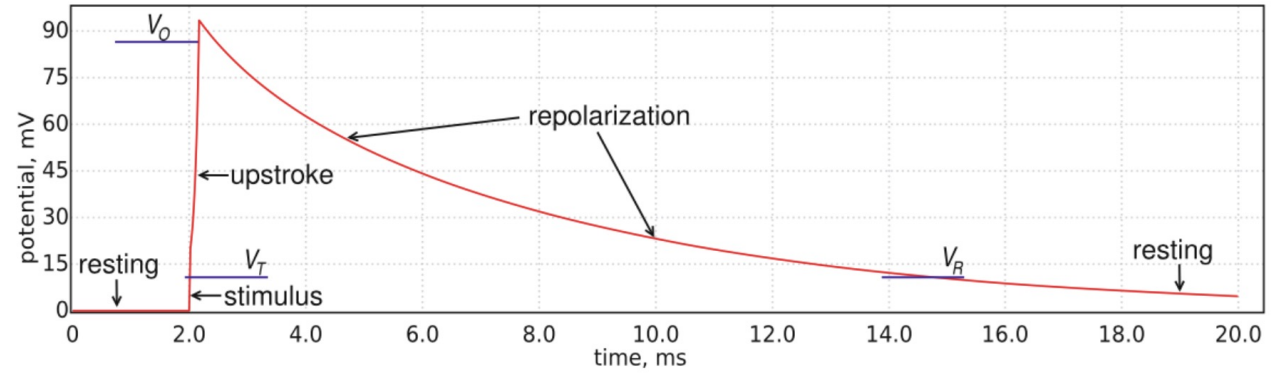


The LRI mode of operation explained



- ▶ LRI (Low Rate Interval) component keeps heart rate above minimum level
- ▶ One of the pacemaker modes of operation that models the basic timing cycle
- ▶ Measures the longest interval between ventricular events
- ▶ Clock reset when VS or VP received
- ▶ No AS received \Rightarrow LRI outputs AP after K (TLRI-TAVI) time units

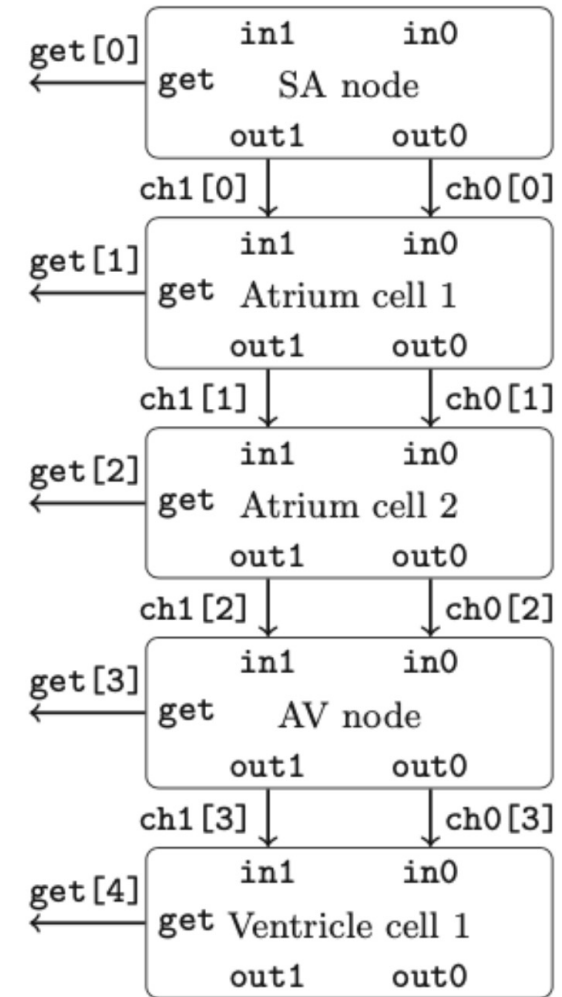
Hodgkin - Huxley model



Hodgkin - Huxley model

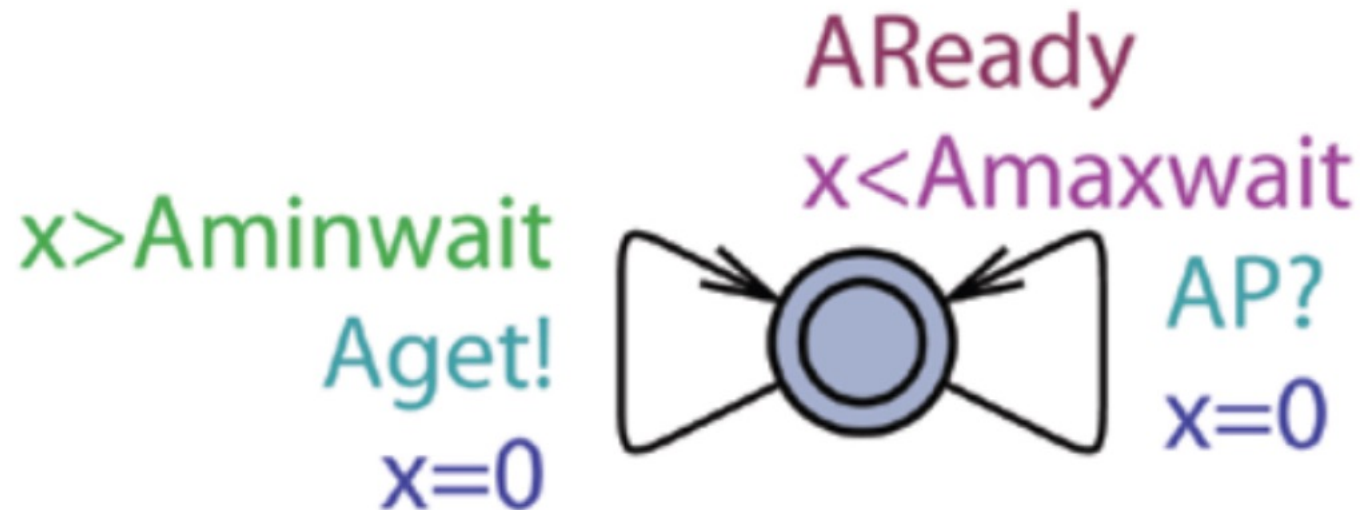
The whole heart model consists of a linear composition of cell models, which synchronize according to their output and input stimuli

At the top of the network, we have the sinoatrial (SA) node: it's input stimulus can come from the natural pacing of the heart or from pacemaker's actuator.



Random Heart Model (RHM)

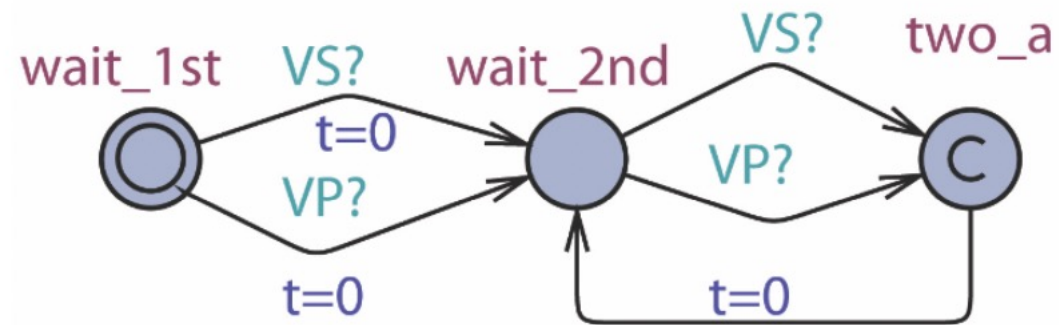
- ▶ RHM is designed to cover open-loop heart behaviors For the atrial region for instance, the interval between each action (*Aget!*) is a random value from the interval (*Aminwait*, *Amaxwait*).



Property

TCTL formula : $A \square ((VS! V VP!) \rightarrow A \square_{\leq TLRI} (VS! V VP!))$

The interval between two ventricular events should be less than TLRI



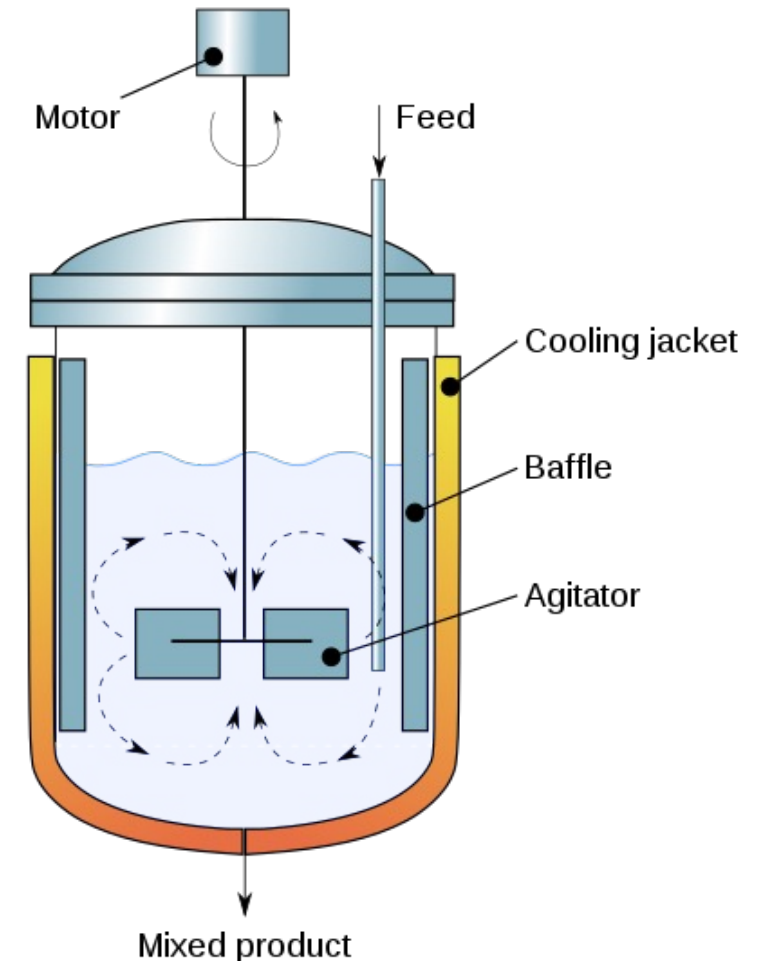
Property

TCTL formula : $A \square (\text{ch1}[0] ! \rightarrow A \diamond \text{ch1}[N] !)$

Given an initial input, the signal should propagate all the way from SA node to atrium and then ventricle, and eventually be visible at the end of the N cells chain described in the previous section.

Temperature Control of a Continuous Stirred Tank Reactor

- Control (PID and MPC) the temperature of an exothermic CSTR so that it follows a constant set point;
- Requirement specification and checking using STL;
- Falsification of the requirements;



Plant Model

First Order Reaction: $A \rightarrow_{k \cdot C_A} B$

Reaction rate per unit volume (Arrhenius law):

$$k(T) = k_0 e^{-E_a/R \cdot T}$$

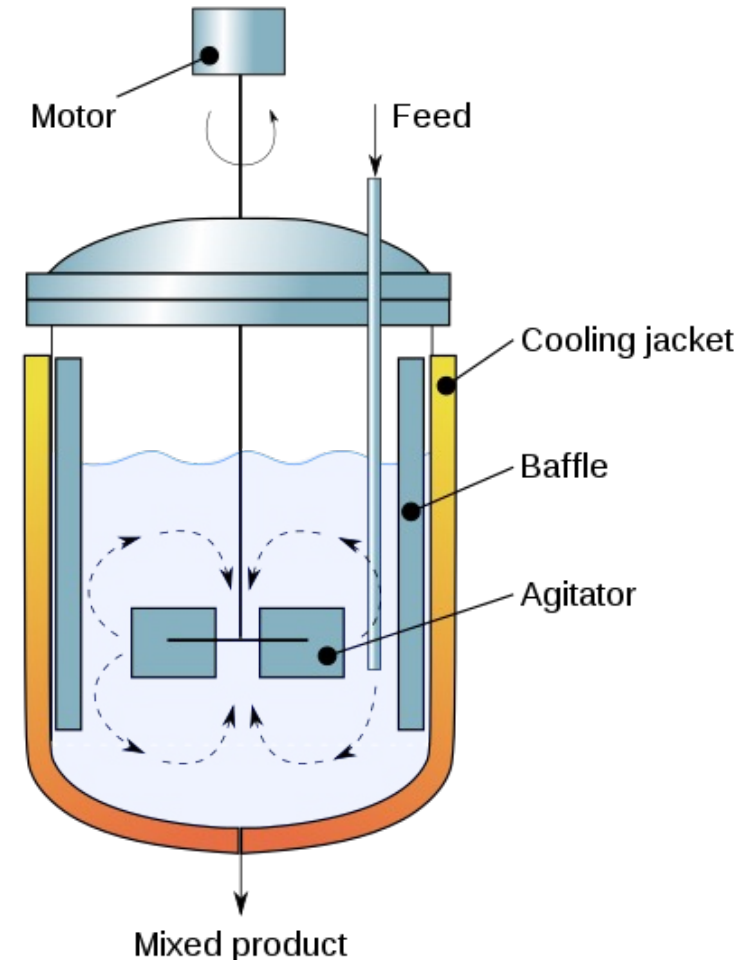
Mole balance equation:

$$\frac{dC_A}{dt} = \frac{q}{V} (C_{Af} - C_A) - k(T)C_A$$

Energy balance equation:

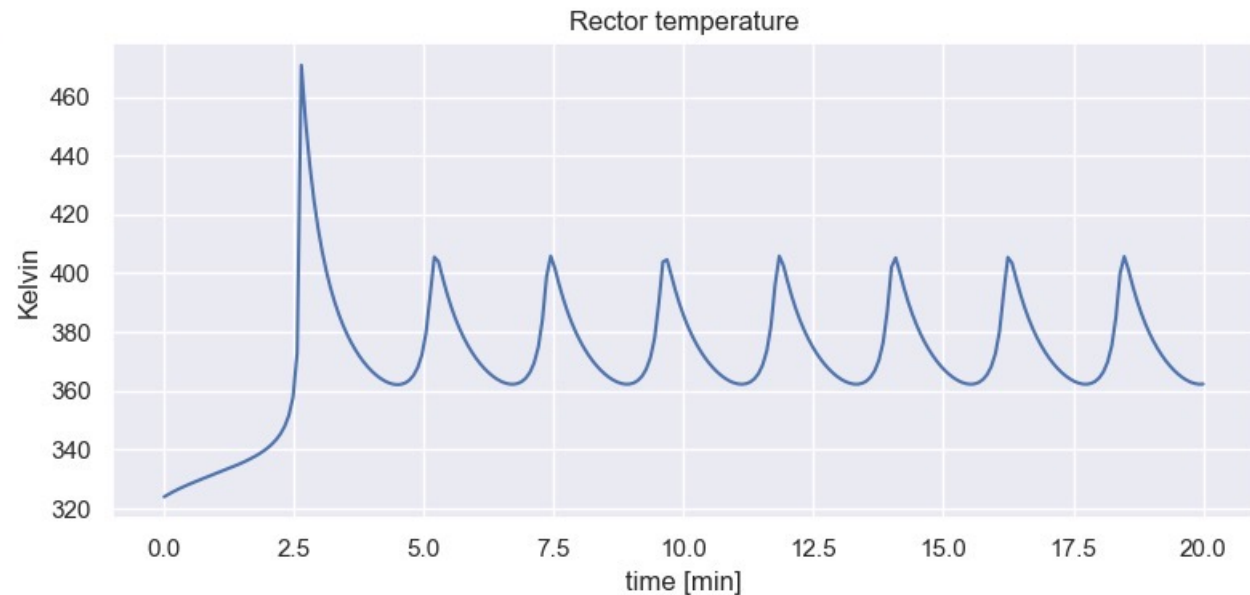
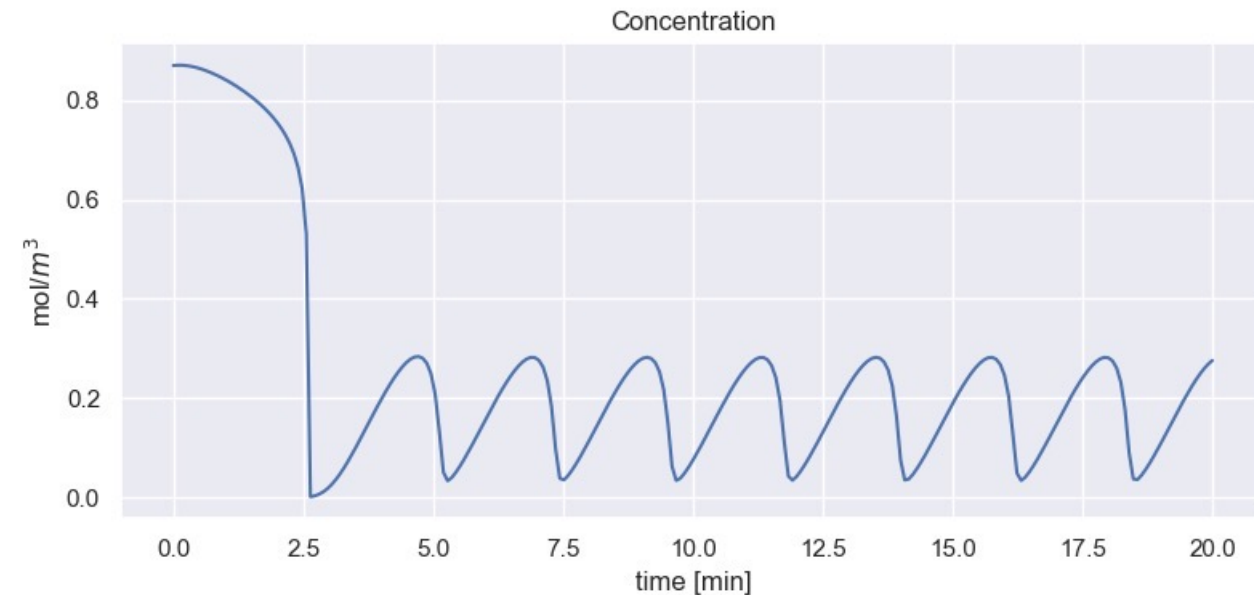
$$\frac{dT}{dt} = \frac{q}{V} (T_f - T) + \frac{-\Delta H_R}{\rho C_p} k(T)C_A + \frac{UA}{\rho C_p V} (T - T_c)$$

Input constraint: $T_c \in [250, 350]$



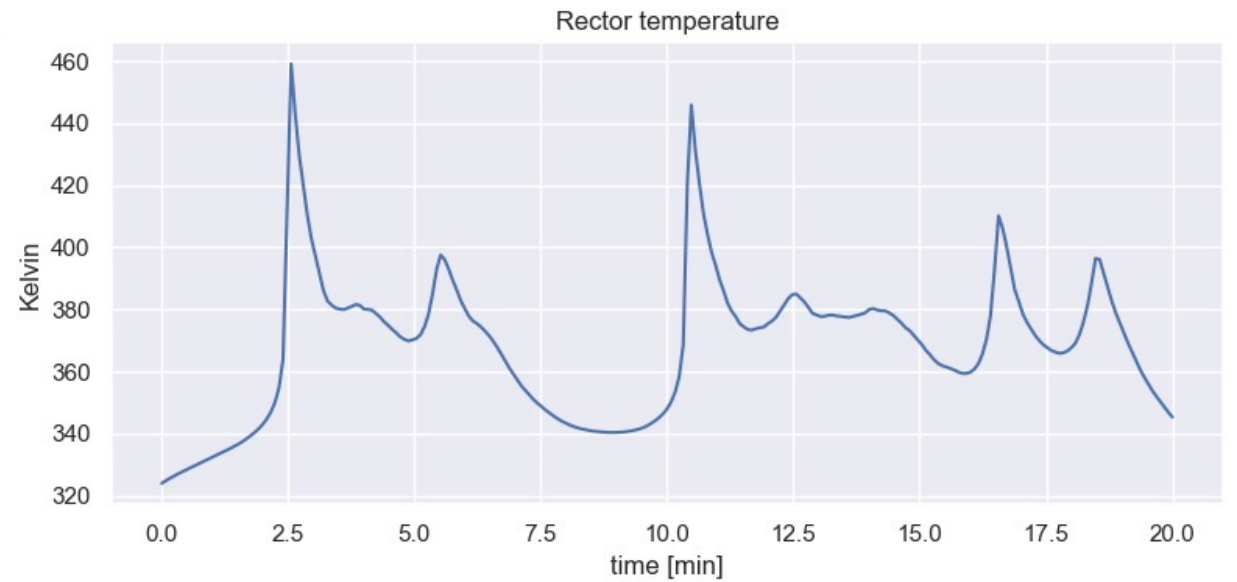
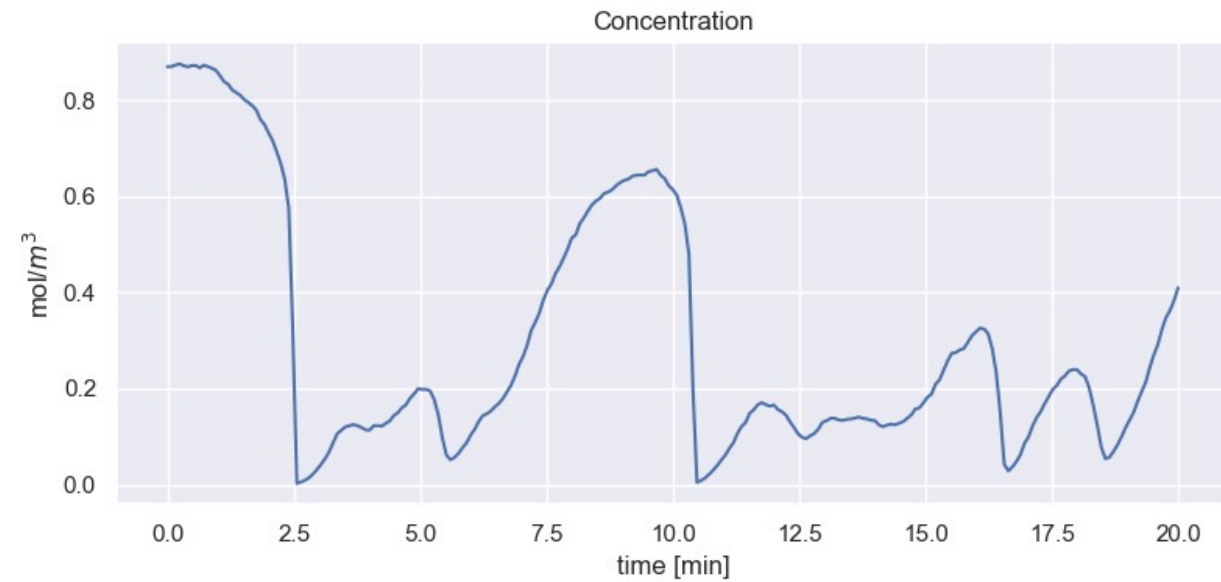
Simulation of the plant

Depending on the reactant A and on the product that we want to obtain, it is desirable that the internal temperature of the reactor T sets to a constant reference value (low if we want concentration of A to be high, and viceversa). However, without any form of control, this cannot be easily achieved, due to the dynamics of the system:



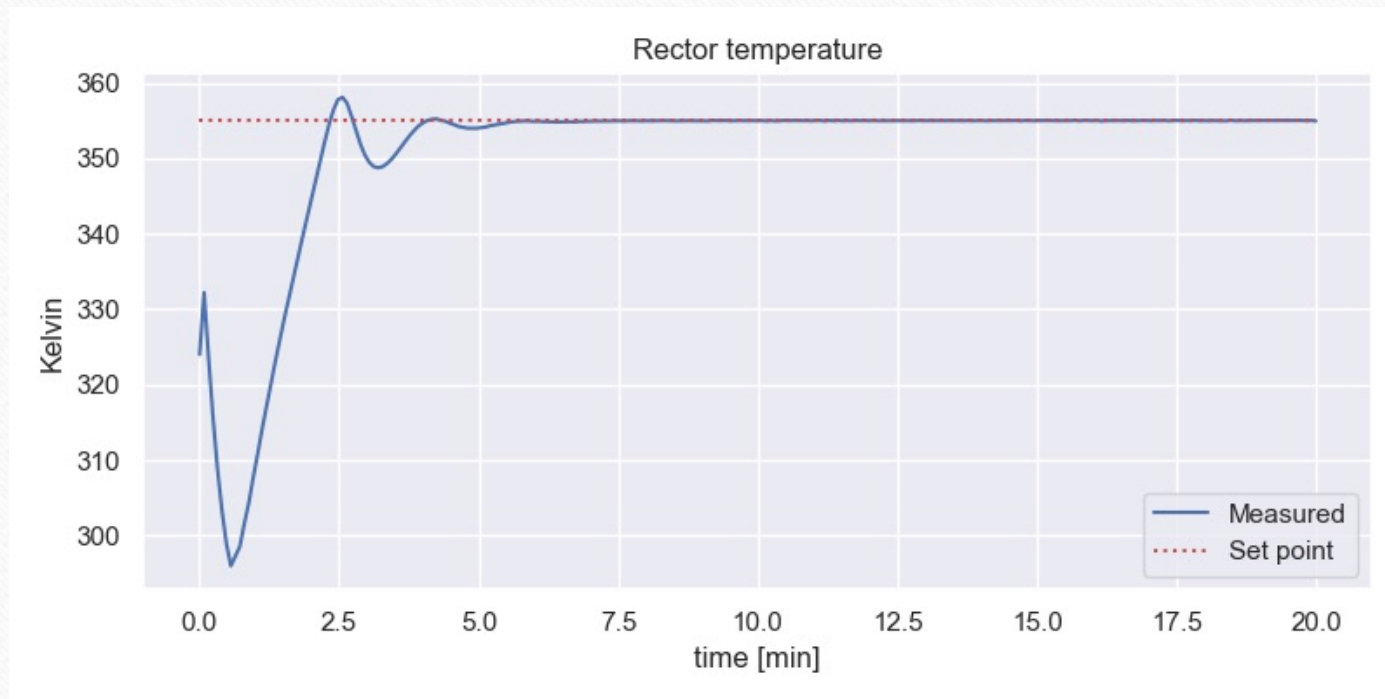
Simulation of the sensor

- ▶ Same as before, but adding Gaussian Noise to observations



PID Control Cont'd

Performance of PID controller when tracking a temperature of 355K



PID parameters:

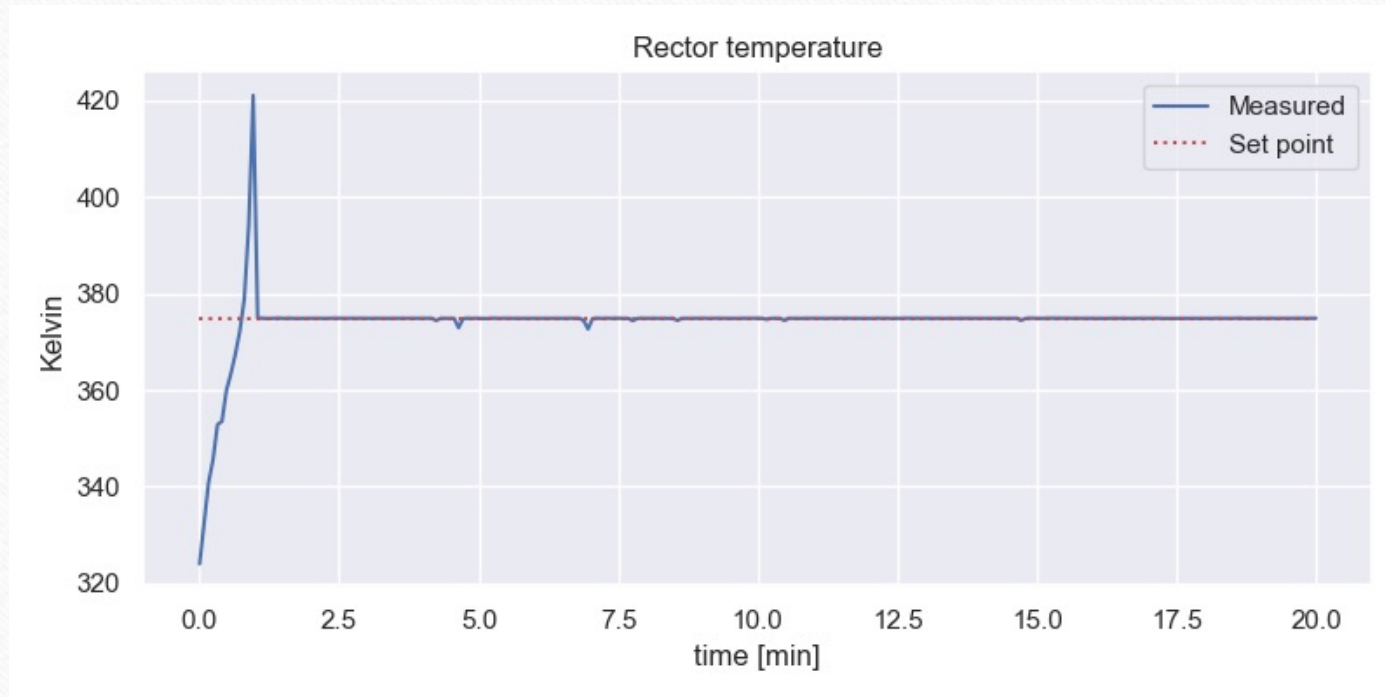
$$K_p = 1.7$$

$$\tau_i = 0.8$$

$$\tau_d = 0.2$$

Non-linear MPC Cont'd

Performance of MPC when tracking a temperature of 375K



MPC parameters:

$$Q = 2.0$$

$$R = 0.01$$

$$H = 10.0$$

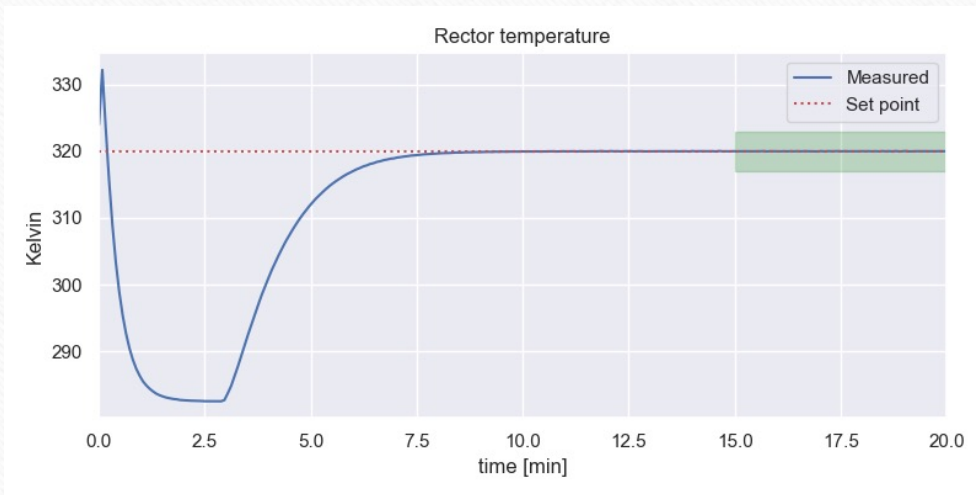
STL Requirements 3

Goal: CSTR should closely follow reference temperature

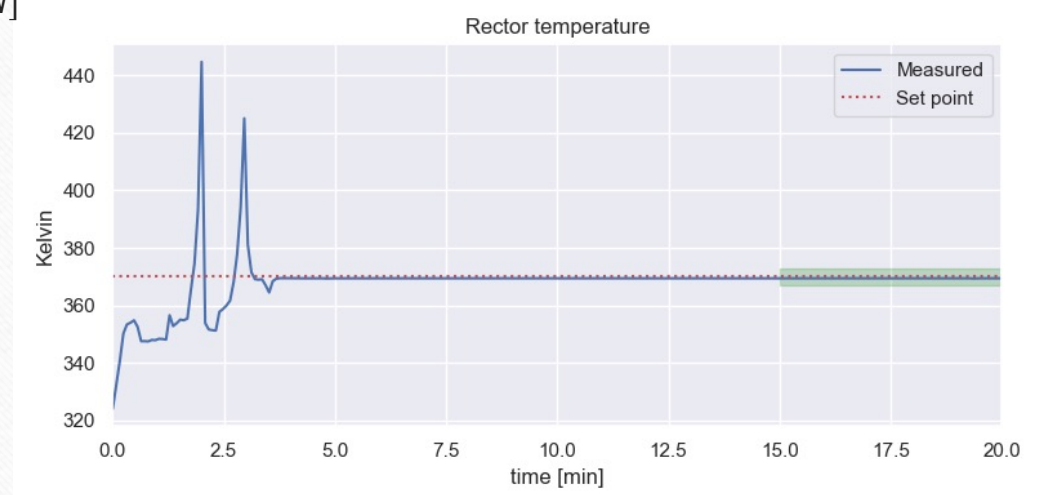
Difference from reference: $d(t) = |T(t) - ref(t)| \forall t$

1. In the last part of the simulation, difference from reference should not exceed $3K$

$$\phi_3 = G_{[\frac{2N}{3}, N]}(d(t) < 3.0)$$



PID

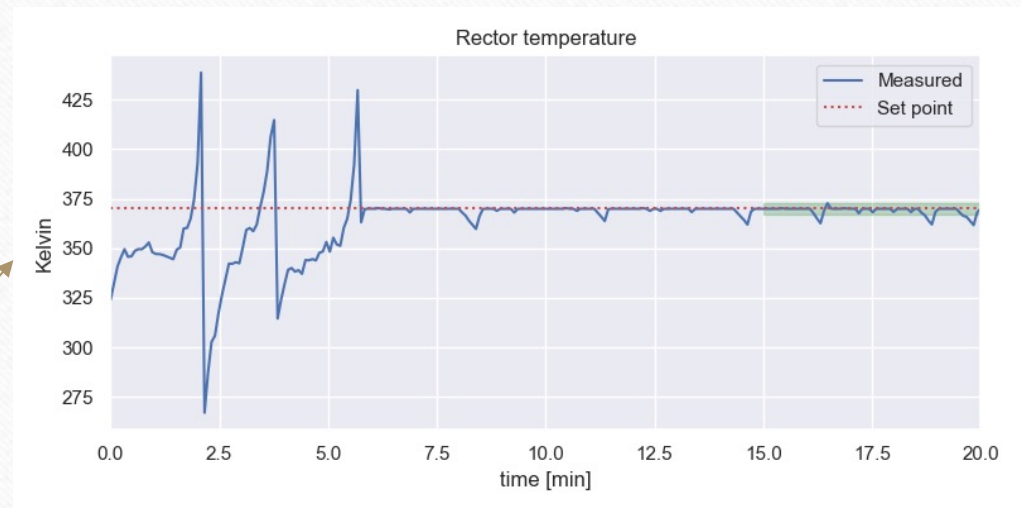


MPC

Falsification Cont'd

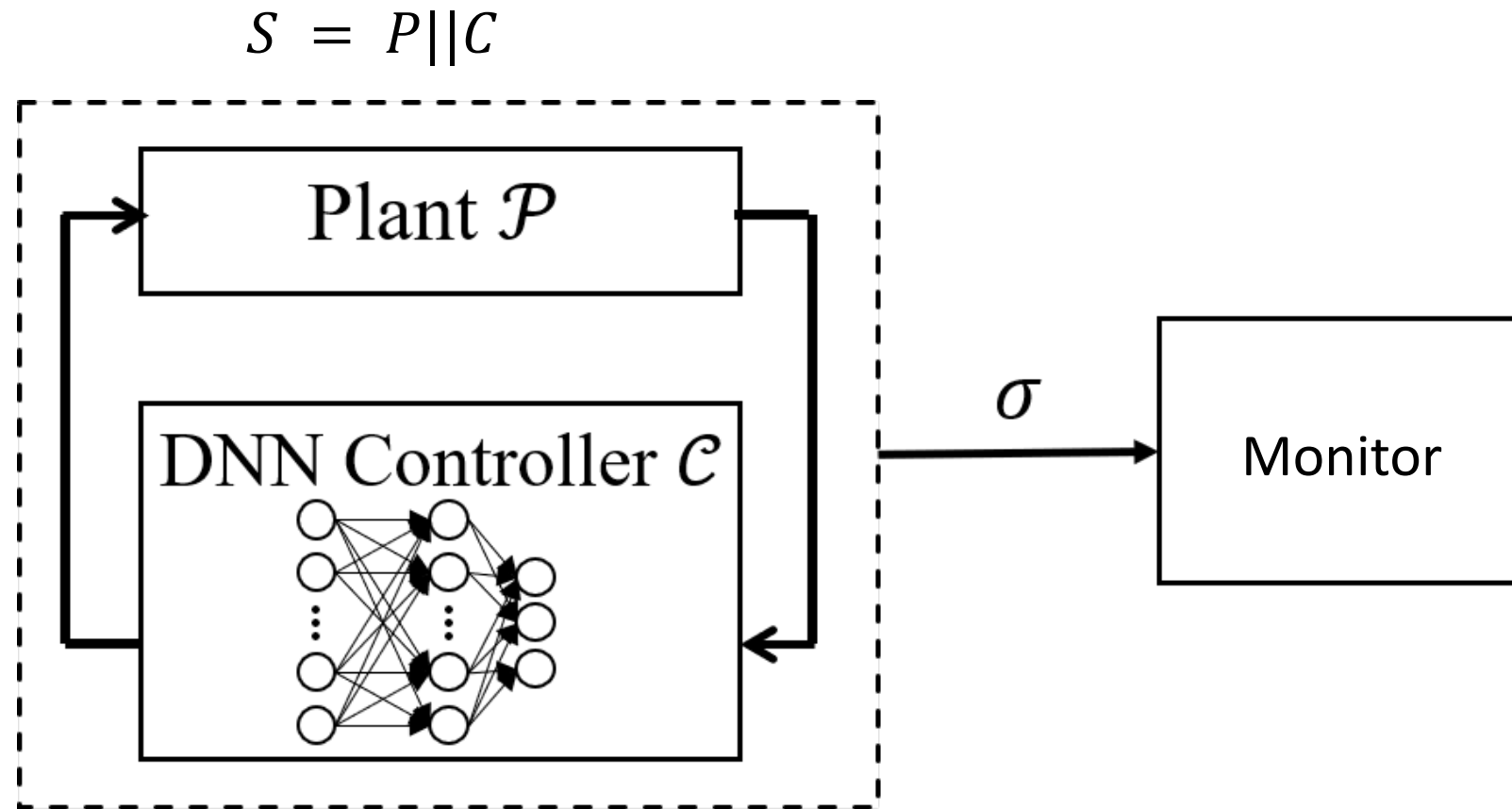
MPC parameters found in falsification analysis

Reference	Q	R	Robustness
320	1.33663	0.020416	-1.28741
325	0.376885	0.024445	-20.7467
330	0.210134	0.0191757	-31.3692
335	1.60591	0.0040131	-0.423672
340	1.63118	0.00144311	-0.0405561
345	2.45878	0.0092065	-0.10704
350	2.67307	0.0045229	-2.28309
355	1.57202	0.00161315	-3.23189
360	1.67468	0.0150942	-8.42903
365	2.70502	0.00979266	-58.8853
370	2.59014	0.00121103	-5.30934
375	1.73716	0.0150608	-0.0113018
380	1.48972	0.018182	-2.94381
385	0.226472	0.0107259	-8.14433



Falsification for reference temperature 370K

A Deep Neural Network controller



Bibliography

Nice survey on Specification-Based Monitoring of CPSs: <http://www-verimag.imag.fr/PEOPLE/maler/Papers/monitor-RV-chapter.pdf>

Artificial Pancreas:

- ▶ Hovorka, R., Canonico, V., Chassin, L.J., Haueter, U., Massi-Benedetti, M., Fed- erici, M.O., Pieber, T.R., Schaller, H.C., Schaupp, L., Vering, T.: Nonlinear model predictive control of glucose concentration in subjects with type 1 diabetes. *Physiol. Meas.* 25(4), 905 (2004)
- ▶ Simone Silveti, Laura Nenzi, Ezio Bartocci, Luca Bortolussi: Signal Convolution Logic. CoRR abs/1806.00238 (2018)
- ▶ F. Shmarov, N. Paoletti, E. Bartocci, S. Lin, S. A. Smolka, and P. Zuliani. Automated synthesis of safe and robust PID controllers for stochastic hybrid systems. arXiv:1707.05229, 2017.
- ▶ Fraser Cameron, Georgios E. Fainekos, David M. Maahs, Sriram Sankaranarayanan: Towards a Verified Artificial Pancreas: Challenges and Solutions for Runtime Verification. *RV 2015*: 3-17
- ▶ Sriram Sankaranarayanan, Suhas Akshar Kumar, Faye Cameron, B. Wayne Bequette, Georgios E. Fainekos, David M. Maahs: Model-based falsification of an artificial pancreas control system. *SIGBED Rev.* 14(2): 24-33 (2017)

Pacemaker:

- ▶ Z. Jiang, M. Pajic, S. Moarref, R. Alur, R. Mangharam, *Modeling and Verification of a Dual Chamber Implantable Pacemaker*, In Proceedings of Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.
- ▶ The textbook has detailed descriptions of some other pacemaker components