Title: Using Formal Methods to Improve Safety of Home-Use Medical Devices

Authors:

Ayan Banerjee	Impact Lab, Arizona State University	**abanerj3@asu.edu**
Yi Zhang	Center for Devices and Radiological Health, US Food and Drug Administration	**Yi.Zhang2@fda.hhs.gov**
Paul Jones	Center for Devices and Radiological Health, US Food and Drug Administration	**Paul.Jones@fda.hhs.gov**
Sandeep K.S. Gupta	Impact Lab, Arizona State University	**Sandeep.Gupta@asu.edu**

Statement of Financial Interest

Ayan Banerjee	*This work of Ayan Banerjee and Dr. Sandeep K.S. Gupta was funded in part by NSF grants CNS-0831544 and IIS-1116385.*
Yi Zhang	N/A
Paul Jones	N/A
Sandeep K.S. Gupta	*This work of Ayan Banerjee and Dr. Sandeep K.S. Gupta was funded in part by NSF grants CNS-0831544 and IIS-1116385.*

Abstract

Advances in technology give rise to increasingly robust and versatile home-use medical devices. Many of these devices are designed to monitor and interact with patients and their physiological systems to help maintain a particular level of health while permitting the patient to be mobile. Unfortunately, there is no well-established *physics* for human physiological systems and their coupling with medical devices. As a consequence, device designers have to resort to gathering empirical data in laboratory or other controlled environments to develop algorithms for approximating physiological systems. This can be expensive, incomplete, and fraught with inherent risks.

Academic research on hybrid automata shows the potential for precisely modeling both the computing aspects of home-use medical devices and their interaction with physiological systems using unified mathematical representations. Formal analysis and *in-silico* simulation can be performed on such representations. This makes possible a more comprehensive and complete assessment on the safety of these devices than traditional approaches.

In this paper, we examine the feasibility and advantages of applying hybrid automata to home-use medical devices, by constructing a non-linear hybrid automaton for a simple artificial pancreas (i.e., closed-loop insulin pump) model. This automaton formalizes the control logic of our artificial pancreas model as a finite state machine and specifies its interaction with the human

glycemic system as differential equations. Our study shows that simulation using this automaton can expose potential design flaws in an artificial pancreas system.

1. Introduction

Advances in technology have enabled the development of novel home-use medical devices to meet society's ever-growing demands for quality healthcare. Many of these devices are designed to work closely with patients by monitoring their physiological conditions to control and deliver appropriate therapy. This type of design, known as closed-loop control, not only facilitates early detection of adverse medical conditions [1, 2], but also enables autonomous decision making for appropriate therapy.

Designs of home-use devices, especially those with closed-loop control, should guarantee: 1) accurate and timely monitoring of patients' physiological condition(s); 2) correct prediction of the patients' needs for therapy; and 3) correct delivery of the predicted therapy. Many of these devices can be quite complex and present varying degrees of risk. It is important that such devices are safe and effective.

Assessing the safety of closed-loop home-use devices presents unique challenges. For example, it requires a profound understanding of the *physics* of human physiology, which is still being discovered. Moreover, the design of home-use devices must account for the patient's rapidly changing environments and varied physiological needs (e.g. change in energy needs moving from walking to running). Current assessment methods rely on experimentation and testing. This is not sufficient, because it only assesses the device under a limited set of scenarios and in controlled environments.

The theory of Hybrid Automata (HA) [11] provides a mathematical means of describing both the continuous and discrete dynamics of complex (closed-loop) control systems, such as those found increasingly in home-use devices. Having such a mathematical representation provides a useful tool for assessing safety properties of these devices, because it allows characterizing these devices, including their functioning mechanisms, discrete control operations, and interaction with patients, into a unified (mathematical) framework. This facilitates automatic analysis, including *in-silico* simulation, that can be performed on HA models to help manufacturers detect design flaws and other safety issues in their devices early in the design phase. More importantly, such analysis enables a more comprehensive assessment of these designs, as compared to current practices, by facilitating the exploration of a much broader set of behaviors from these designs.

In this paper, we demonstrate the usefulness of HA in home-use medical device design, by applying it to a relatively simple, yet generic, artificial pancreas (AP) (i.e., closed-loop insulin infusion pump) design. The focus of our study is to assess the safety of the control strategy underlying this design. We construct a non-linear HA model (that includes interaction with patients). Time-bounded simulations were performed on this model. Simulation results revealed that this design might cause hypo / hyperglycemia in diabetic patients.

2. Artificial Pancreas Systems

AP devices [3] are a good example of home-use devices with closed-loop control. Several novel AP (control) systems have been proposed and many are under clinical study. Most AP devices utilize one or more Continuous Glucose Monitor (CGM) sensors [5] to constantly measure the patient's BG level. This provides a basis for determining the amount of insulin (in the single hormone systems) or insulin and glucagon (in the bi-hormonal systems) to be delivered. Current AP devices use a variety of controllers, including PID controllers [6], fuzzy logic controllers [7], and model predictive controllers [8].

In this paper, we consider a simple yet representative AP design (Figure 1)[1], which comprises:

- An insulin pump, which provides continuous (or near continuous) delivery of insulin.
    - Insulin delivered throughout the day to meet the patient's variable background metabolic need is referred to as the basal insulin.
    - Insulin delivered to address meals (carbohydrate intake) is referred to as the pre-prandial bolus insulin;
- A CGM sensor, which continuously monitors the patient's interstitial glucose level and reports it to a remote receiver via wireless communication.
- A remote computer-based controller. For example, the system receives interstitial glucose values from the CGM sensor and the controller processes these values through a simple Kalman filter [8] to predict the patient's blood glucose in the near future if the current insulin delivery rate remains unchanged. If the predicted future blood glucose level exceeds the programmed bounds (lower and upper), the controller instructs the insulin pump to adjust the insulin delivery rate accordingly.

More specifically, the controller uses a supervisory control algorithm to adjust insulin administration to keep the patient's BG level within a pre-specified safe range. The control algorithm decomposes the operation of the insulin pump into three discrete modes:

i) *Braking*: This mode continuously adjusts the basal rate based on the level of risk implied by the projected BG level. The risk level, *R(t)*, implied by a future BG level is calculated as follows: if the BG level after one hour, denoted as $BG_{60\min}$, >= 120 mg/dl, *R(t)* is set to 0; if $BG_{60\min}$ <= 20 mg/dl, *R(t)* is set to 100; otherwise, *R(t)* is calculated as a non-linear logarithmic function of $BG_{60\min}$. The basal rate is then reduced by a fraction proportional to *R(t)*.

ii) *Meal Supervision*: The system transitions into this mode if it is currently not in the *Braking* mode and the patient is about to have a meal. Upon entering this mode, the control algorithm allows the patient to indicate the meal size (from three options), and then computes the dosage of insulin needed to compensate for the meal accordingly.

---

[1] This model was first proposed in [8]. The sole reason for using the AP model in our study is to show the potential use of HA in home-used medical device design verification. For some recent advances in AP technology, see for example [12].

iii) *Correction Bolus*: The system transitions into this mode only when all of the following conditions hold: 1) it has been more than two hours since the last meal bolus, 2) it is not currently in the *Braking* mode, 3) at least one hour has passed since the last correction bolus, and 4) $BG_{60\,\mathrm{min}}$ is predicted to be greater than 180 mg/dl. In this mode, a correction bolus is delivered to the patient, the size of which is calculated as a linear function of $BG_{60\,\mathrm{min}}$.

3 Modeling Artificial Pancreas with Hybrid Automata

Hybrid Automata. A *HA* consists of a finite set of discrete states and transitions among them, where each state contains a set of variables and each transition is labeled with a condition on the variables (of the source state). Each state of a HA is also defined with a set of differential equations to govern the values of variables in it. If all differential equations in a HA are linear, i.e., taking the form of $dv/dt = Av + B$, this automaton is linear.

Given a HA *A*, each of its executions starts from its initial state with a distinct initial condition, which defines the values of *A's* variables at the beginning of the execution. As the execution proceeds, the differential equations in *A*'s current state are solved to update the values of all involved variables. These values are then used to evaluate the conditions labeled on transitions outgoing from *A*'s current state. If any of such conditions is satisfied, the automaton takes the transition and enters into its destination state. Notably, entering into a new state can cause a new set of differential equations to be solved in the future, reflecting the changes in system dynamics.

Modeling Patient Insulin-Glucose Reaction. Formalizing the example AP design in Section 2 requires modeling the CGM sensor as well. However, if the focus is to evaluate the safety and correctness of the control strategy embedded in this design, then the engineering details of the CGM sensor can be replaced by a patient physiological model, such as Bergman Minimal Model (BMM) [9].

The BMM defines the interaction between insulin and the patient's blood glucose (either stored internally or provided through meals) as a set of non-linear ordinary differential equations, as illustrated in Equation 2, where *G(t), X(t),* and *I(t)* are the patient's BG level, and interstitial and plasma insulin concentration, respectively. In addition, in Equation 2, $k_1, k_2, k_3, k_4, k_5, k_6, I_b,$ and G_b are patient-specific constants, derived either from empirical data or using diabetic patient simulators [10].

$$\begin{aligned}
\frac{dX(t)}{dt} &= -k_2 X(t) + k_3 (I(t) - I_b) \\
\frac{dG(t)}{dt} &= -X(t) \bullet G(t) + k_1 (G_b - G(t)) \\
\frac{dI(t)}{dt} &= -k_4 I(t) + k_5 (G(t) - k_6) t
\end{aligned} \tag{2}$$

The example AP design also needs input from the patient to indicate the timing and size of meal intakes. We adopt a zero mean Gaussian random process to model the patient's dietary behavior, where we assume the meal size, *w(t)*, can only take values from the set {0,2.5,3,5}, as a way to abstract potential meal sizes for the sake of simplicity.

Construct HA model for Artificial Pancreas. The HA model constructed for the example AP design contains three discrete states, each corresponding to one of the aforementioned operational modes. An additional state is introduced to represent basal infusion. Figure 2 depicts the structure of the model, in which each state shares a same set of variables, including *X(t)*, *G(t)*, and *I(t)*. All these variables are governed by Equation 2.

This automaton always starts execution from the *Basal Infusion* state, and then transits to other states based on corresponding transition conditions: It transits to the *Braking* state when $BG_{60\min}$ is predicted to be less than 120 mg/dl, and returns back if it becomes greater; the transition to the *Meal Supervision* state is triggered if a meal is taken (*w(t)* > 0), and the automaton exits from this state after two hours ($\tau > 120\,\text{mins}$); the automaton starts a correction bolus if $BG_{60\min}$ is greater than 180mg/dl, and resumes the basal infusion one hour after.

4. Analyzing Hybrid Automata

In-silico HA models have been very useful in testing algorithms to ensure that they run appropriately and permit the investigator to test the range of parameters that the algorithm can handle. For example, simulating a HA model can reveal, to the extent permitted by simulation time and initial conditions, the presence of unsafe states. While *in-silico* models have allowed us to decrease the reliance on animal testing and allowed some decrease in developmental time we have found that the algorithms generally have to be adjusted once testing with human subjects has begun. These models appear to be useful in the initial stages of system development but are not sufficient to test the range of dynamic changes and demands that are unique to each patient[2]. Therefore, the current models would not obviate the need for well-designed clinical studies to evaluate the final system.

We used the Breach package from the MATLAB® tool suite [4], to simulate the HA model presented in section 3. Breach is a simulation and verification tool for analyzing dynamic systems with non-linear differential equations. Using Breach, we can establish desired safety boundaries and then see if the treatment boundary is exceeded. We used a generally acceptable lower boundary of 60 mg/dl[3] and upper boundary of 250 mg/dl; recognizing that there are no hard thresholds that hold across all possible cases and that simulation of individual cases are likely warranted.

The time bound for the simulation was set as 10000 seconds, and the initial states of the simulation were defined as $\{ X(t), G(t), I(t) \}$ = {[0, 0.1], [60, 180], [0, 100]}. Figure 3 illustrates the portion of state space explored during the simulation (shown as the shaded regions). As Figure 3 reveals, the model might lead diabetic patients into harmful situations such

[2] This is especially true for type-1 diabetic patients as potential users of AP devices. They usually demonstrate great diversity in internal glycemic systems, reaction to insulin, and personal behavior patterns, which require treatment plans unique to each individual patient.

[3] 60 – 70 mg/dl is a common lower bound for an average patient. We used 60 mg/dl for our research.

as hypoglycemia, because unsafe states (regions beyond the red threshold) were reached during the simulation.

Simulation on HA models can expose the presence of design errors if appropriate simulation time and initial conditions are selected. Developers will still need to establish the cause(s) of these errors with appropriate corrections.

It is possible to analyze HA models more comprehensively using mathematical-based verification techniques such as those described in [13]. The reason we chose simulation to analyze the HA model lies in the nonlinearity of the model. Complex systems such as human physiological systems typically demonstrate certain nonlinearities, i.e., the system output is not directly proportional to the input. Thus, the HA models constructed for these systems are nonlinear (see Equation 2 for instance). Mechanical reasoning of these models requires finding closed-form solutions for their non-linear differential equations, which is often computationally expensive, and sometimes impossible.

5. Discussion

This preliminary study applies the HA technique to a simple AP design. Many challenges, both technical and theoretical, have to be addressed when the HA technique is applied to real-world, complex devices. For example, to model realistic AP systems one has to consider noise factors and errors from CGMs measurements, diffusion delay of insulin in subcutaneous tissues, predictive models of human activities and physiology, etc. Failing to address these issues may result in significant discrepancies between a HA model and a real world system. The delta between model and real-world properties can be reduced through principled collaborations between designers and HA and domain experts. However,, there will likely always be a delta in properties between a real device and its HA model. Thus, system-level validation and clinical experimentation are still necessary to account for this fact.

A challenge limiting the applicability of HA models in closed-loop medical devices is the so-called *state space explosion* phenomenon. For a complicated control system, its corresponding HA model can contain a large number of variables. Consequently, the state space of the model can be too large to handle. For example, the Kalman filter in section 2 computes the predicted BG level as a linear function of previous BG values. Modeling this predictor requires a large set of variables to store historic BG readings, since HA models are memory-less [11]. One solution to this issue is to convert equations that imply a large state space into continuous differential equations. The tradeoff of this solution, however, is potential discrepancies between the model and the "real world" system.

6. Conclusions

In this paper, we used a simple artificial pancreas design as an example to show that the hybrid-automata framework can be used to characterize and analyze the design of closed-loop devices. This work only constitutes a first step of our effort toward using hybrid automata to assess and

improve the safety of (home-use) closed-loop medical devices. Future work might include a) applying hybrid automata techniques to more complex AP models or b) investigating additional verification techniques, such as reachability analysis for hybrid automata models; which may enable a more comprehensive assessment of home use device safety.

Figures

Figure 1. An Example Artificial Pancreas System

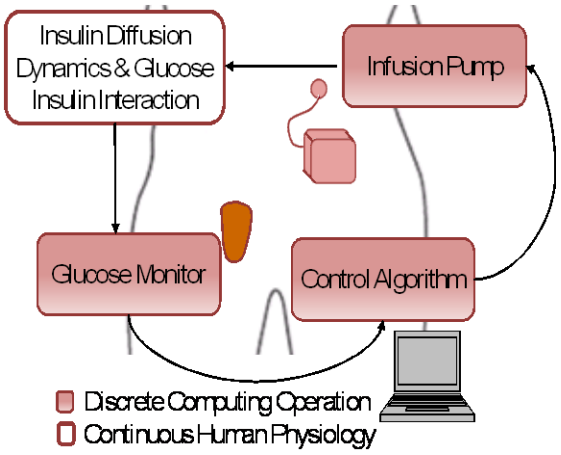


Figure 2. Artificial Pancreas Hybrid Automaton Model

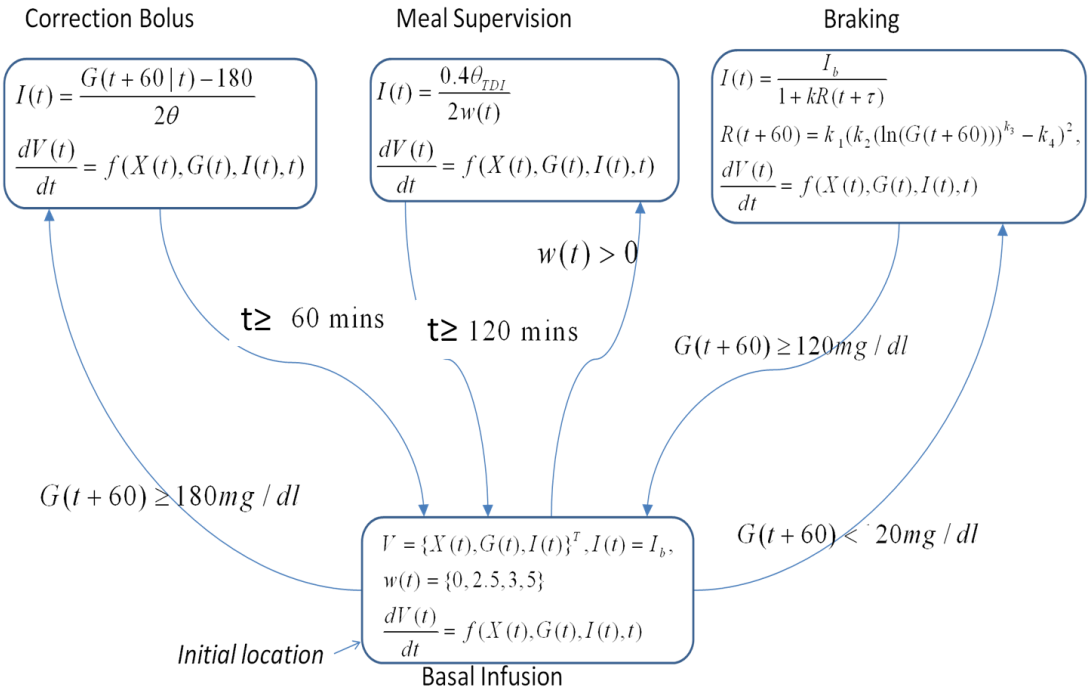
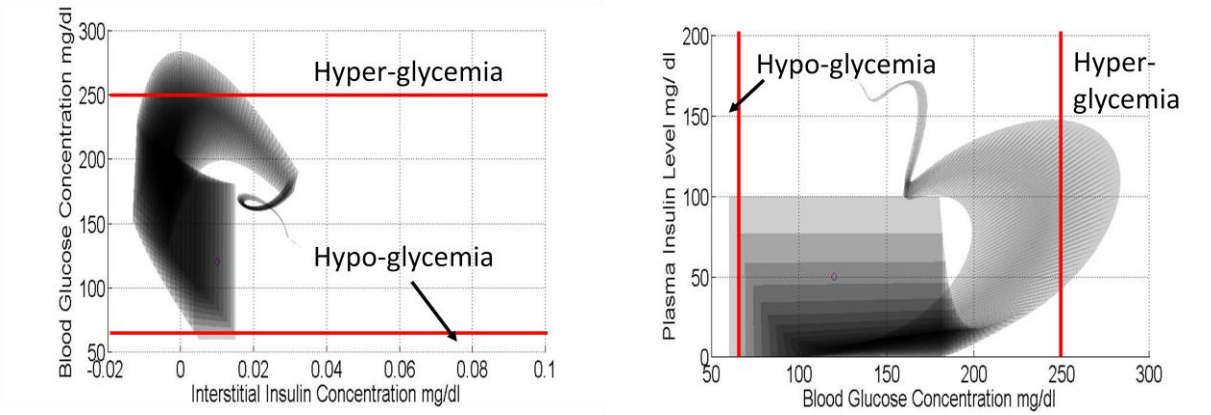


Figure 3. Simulation Results for AP HA Model



REFERENCES

[1] Stern S and Tzivoni D. *Early detection of silent ischaemic heart disease by 24-hour electro-cardiographic monitoring of active subjects.* British Heart Journal, volume 36, issue 5, pages 481-6, May 1974.

[2]http://iuhealth.org/methodist/neuroscience/technology/neuromonitoring/

[3]http://articles.latimes.com/2012/jun/12/science/la-sci-sn-artificial-pancreas-gives-diabetics-a-break-20120609

[4] Donze A, *Breach, a toolbox for verification and parameter synthesis of hybrid systems.* In proceedings of the 22nd international conference on Computer Aided Verification (CAV'10), pages 167-170, Jul. 2010.

[5] Castle JR, Pitts A, Hanvan K, Muhly R, El Yossef J, Hughes-Karvetski C, Kovatchev B, Ward WK. *The accuracy benefits of multiple amperometric glucose sensors in people with type 1 diabetes.* Diabetes Care, volume 35, issue 4, pages 706-10, Apr. 2012.

[6] Marchetti G, Barolo M, Jovanovic L, Zisser H, Seborg DE. *An improved PID switching control strategy for type 1 diabetes.* IEEE Transactions on Biomedical Engineering, volume 55, issue 3, pages 857-65, Mar. 2008.

[7] Yasini S, Naghibi-Sistani MB, Karimpour A. *Active insulin infusion using fuzzy based closed loop control.* In proceedings of the 3rd IEEE international conference on Intelligent System and Knowledge Engineering (ISKE'08), volume 1, pages 429-434, Nov. 2008.

[8] Kovatchev B, Patek S, Dassau E, Doyle FJ 3rd, Magni L, De Nicolao G, Cobelli C. *Control to range for diabetes: functionality and modular architecture*. Journal of Diabetes Science and Technology, volume 3, issue 5, pages 1058-65, Sept. 2009.

[9] Bergman minimal model - http://www.civilized.com/mlabexamples/glucose.htmld/

[10] T1DM simulator - http://www.tegvirginia.com/T1DM.htm

[11] A. Girard and G. J. Pappas, "Verification using simulation," in Hybrid Systems: Computation and Control (HSCC), ser. LNCS, vol. 3927. Springer, 2006, pp. 272–286.

[12] Patek S.D., Magni L., Dassau E., Hughes-Karvetski C., Toffanin C., DeNicolao G., Del Favero S., Breton M., Man C.D., Renard E., Zisser H., Doyle F.J., Cobelli C, Kovatchev B.P. *Modular Closed-Loop Control of Diabetes*, IEEE Transaction on Biomedical Engineering, vol. 59, no. 11, pp. 2986-2999, Nov. 2012.

[13] Alur R., *Formal verification of hybrid systems*, in proceedings of the International Conference on Embedded Software, pp.273-278, Oct. 2011