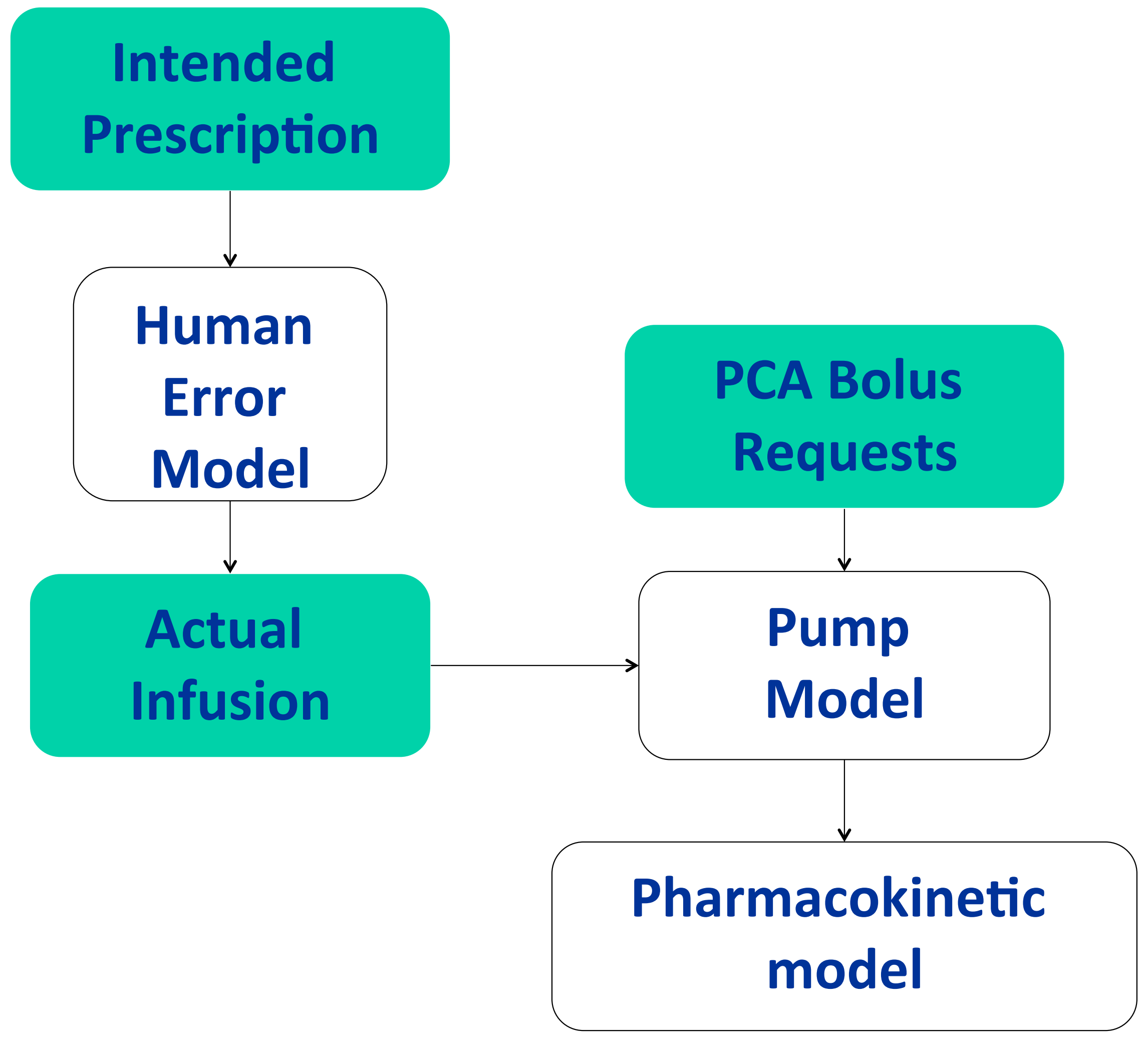
Formal Dependability Analysis for Real-Time Medical Devices.

Sriram Sankaranarayanan, Clayton Lewis and Hadjar Homaei
University of Colorado, Boulder, CO, USA.

Infusion pumps are commonly used in home/hospital care to deliver drugs to patients at programmable rates over time. Their use involves numerous risks due to human and machine faults that can cause serious harm to the patient. We present a framework for formally modeling human errors and machine faults that may occur during an infusion. Our framework can provide quantitative predictions of the worst case effects on the patient using verification techniques. Our work can be used as an overall framework for risk analysis due to human and machine faults.

Figure 1. Commercial Infusion Pump Models.



Intended Prescription

Human Error Model

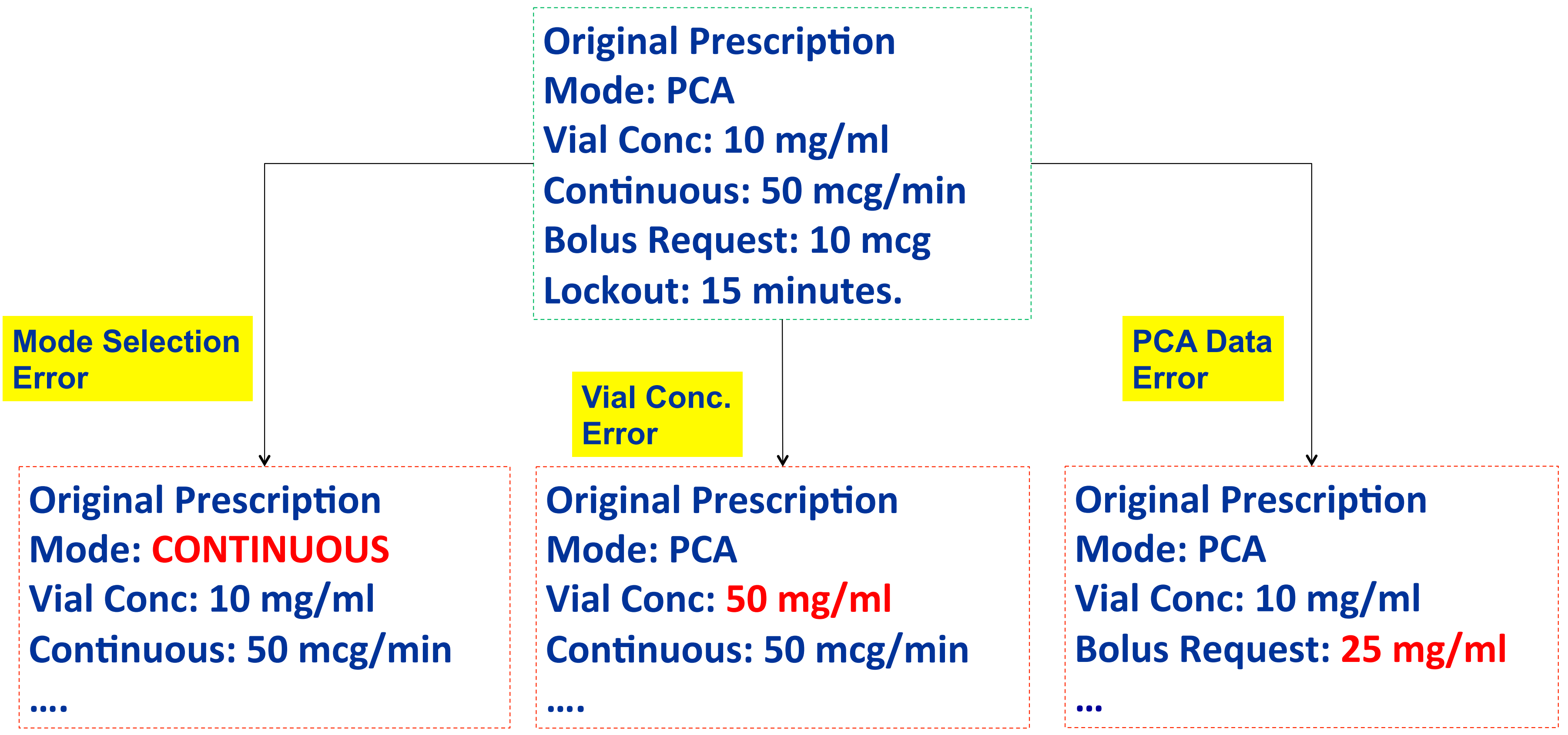
Actual Infusion

PCA Bolus Requests

Pump Model

Pharmacokinetic model

Figure 2. Basic components of the infusion model.



Original Prescription
Mode: PCA
Vial Conc: 10 mg/ml
Continuous: 50 mcg/min
Bolus Request: 10 mcg
Lockout: 15 minutes.

Mode Selection Error

Vial Conc. Error

PCA Data Error

Original Prescription
Mode: CONTINUOUS
Vial Conc: 10 mg/ml
Continuous: 50 mcg/min
….

Original Prescription
Mode: PCA
Vial Conc: 50 mg/ml
Continuous: 50 mcg/min
….

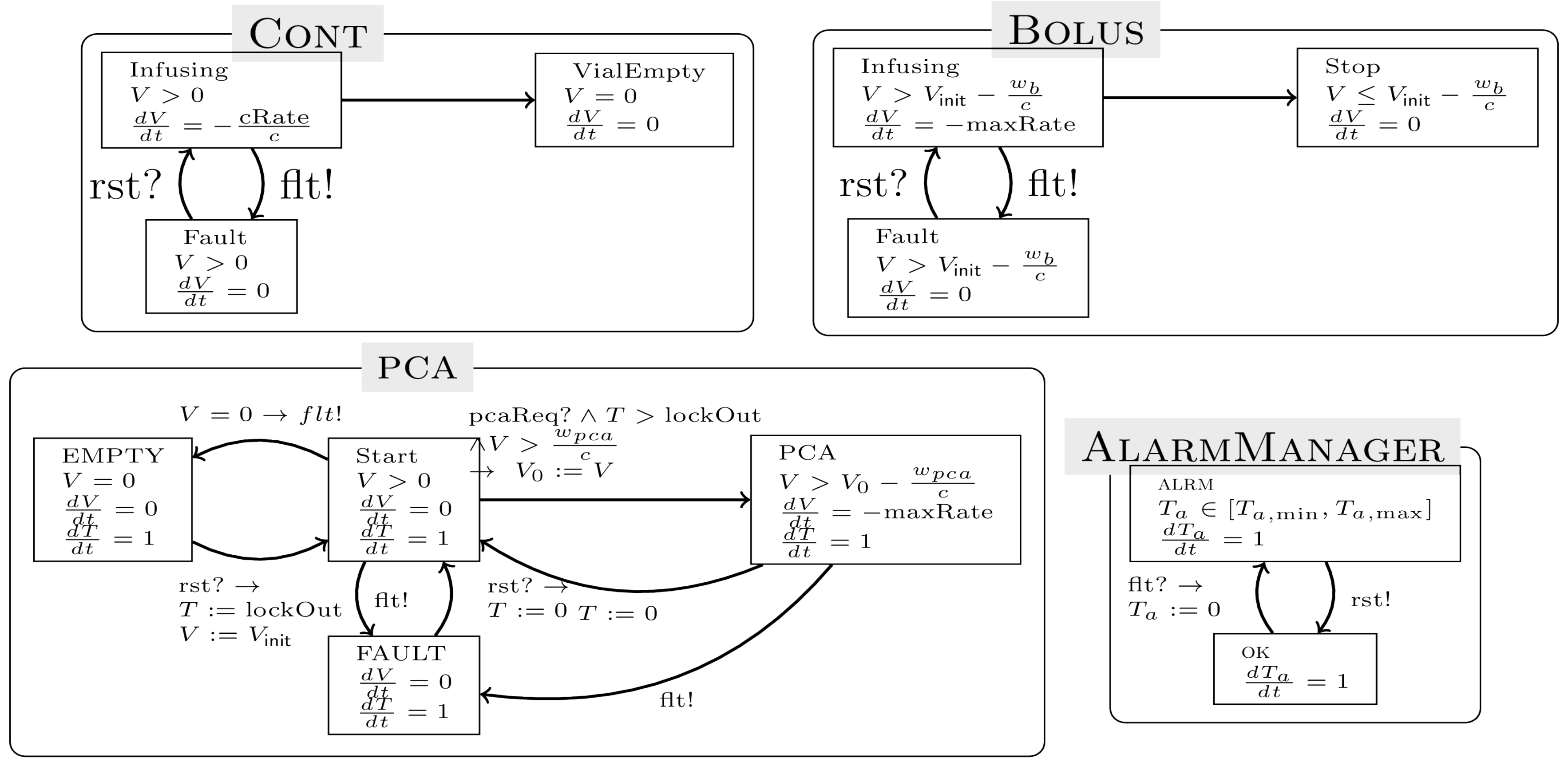
Original Prescription
Mode: PCA
Vial Conc: 10 mg/ml
Bolus Request: 25 mg/ml
…

Figure 3. Human error model as a transformation from intended to actual prescription.

Modeling Framework

Our work employs a detailed modeling framework that comprises of three basic models:

- **Human error model** captures possible mistakes committed by the operator programming the infusion during an interaction.
- **Pump model (hybrid automaton)** captures the pump operation in response to the programmed infusion.
- **Pharmacokinetic model (ordinary differential equations)** captures the diffusion of the drug through the patient's blood stream and other parts of their body.

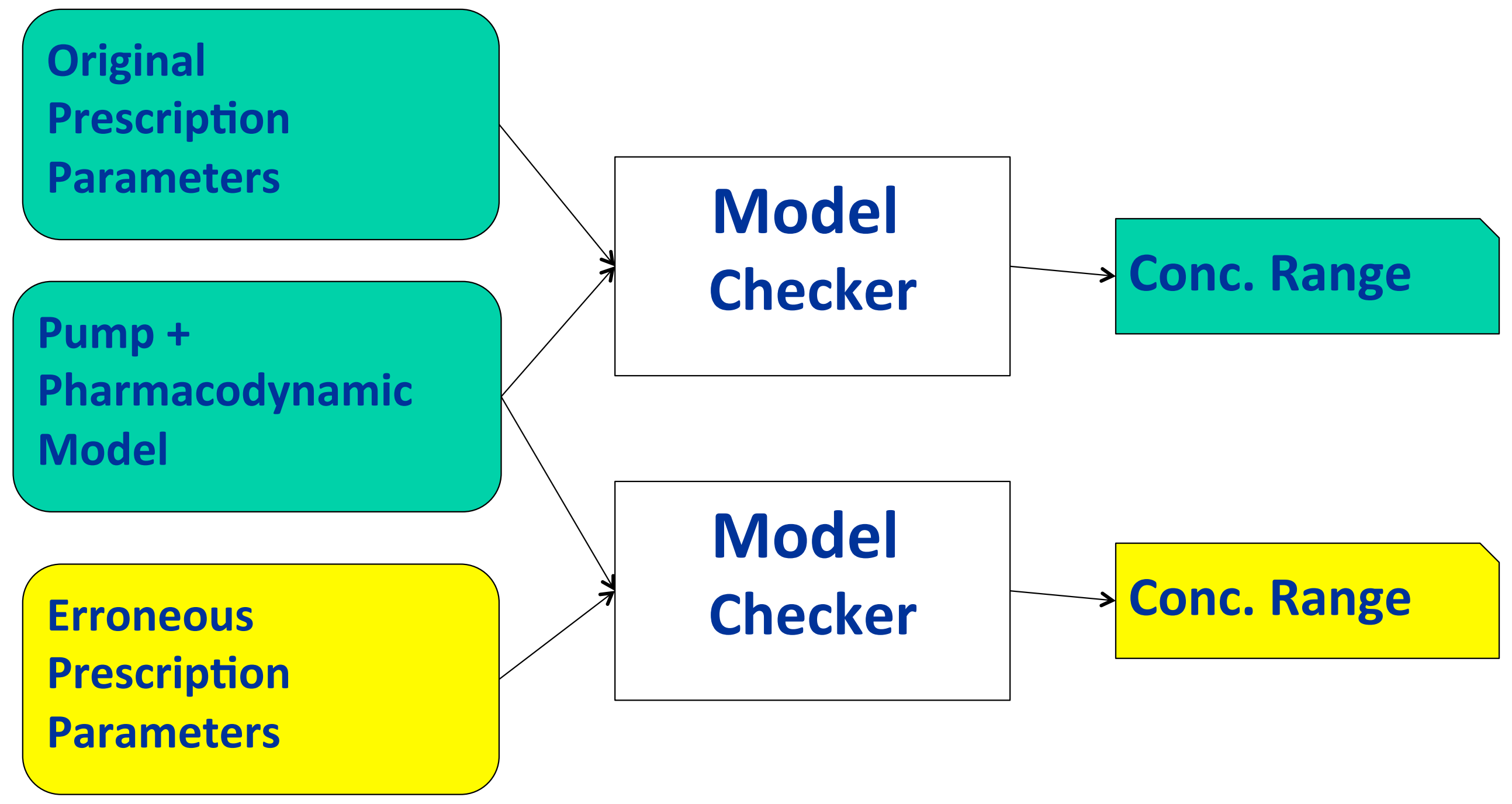


CONT
Infusing $V > 0$ $\frac{dV}{dt} = -\frac{\text{cRate}}{c}$
VialEmpty $V = 0$ $\frac{dV}{dt} = 0$
rst?
flt!
Fault $V > 0$ $\frac{dV}{dt} = 0$
BOLUS
Infusing $V > V_{\text{init}} - \frac{w_b}{c}$ $\frac{dV}{dt} = -\text{maxRate}$
Stop $V \leq V_{\text{init}} - \frac{w_b}{c}$ $\frac{dV}{dt} = 0$
rst?
flt!
Fault $V > V_{\text{init}} - \frac{w_b}{c}$ $\frac{dV}{dt} = 0$
PCA
$V = 0 \rightarrow flt!$
EMPTY $V = 0$ $\frac{dV}{dt} = 0$ $\frac{dT}{dt} = 1$
Start $V > 0$ $\frac{dV}{dt} = 0$ $\frac{dT}{dt} = 1$
pcaReq? $\wedge\, T >$ lockOut $\wedge\, V > \frac{w_{pca}}{c} \rightarrow V_0 := V$
PCA $V > V_0 - \frac{w_{pca}}{c}$ $\frac{dV}{dt} = -\text{maxRate}$ $\frac{dT}{dt} = 1$
rst? $\rightarrow$ $T :=$ lockOut $V := V_{\text{init}}$
flt!
rst? $\rightarrow$ $T := 0$ $T := 0$
FAULT $\frac{dV}{dt} = 0$ $\frac{dT}{dt} = 1$
flt!
ALARMMANAGER
ALRM $T_a \in [T_{a,\min}, T_{a,\max}]$ $\frac{dT_a}{dt} = 1$
flt? $\rightarrow$ $T_a := 0$
rst!
OK $\frac{dT_a}{dt} = 1$

Figure 4. Pump Model Components.

Analysis Framework

The composed models form a hybrid automaton with affine dynamics. We use standard model checking tools to predict the range of possible concentration of the infused drug in the patient's bloodstream.



Original Prescription Parameters

Pump + Pharmacodynamic Model

Erroneous Prescription Parameters

Model Checker

Model Checker

Conc. Range

Conc. Range

Figure 5. Analysis Framework for comparing the effect of human errors.

Evaluation

We have implemented the analysis framework in OCaml using bounded model checker for hybrid automata. Case study inspired by Generic Infusion Pump Model (GIP). Worst case scenarios with quantitative predications were obtained. These scenarios are in line with real-life accidents involving infusion pumps.

Ongoing Work

Infusion pump modeling framework allowing detailed models of the interface and the possible human mistakes. Automatic user-error detection mechanisms for infusion pumps.

References

[1] **Sankaranarayanan et al.** *Model-based analysis of real-time medical devices*, **Formal Modeling and Analysis of Timed Systems (FORMATS) 2011 .**

[2] **Arney et al.** *Generic Infusion Pump: Hazard Analysis and Safety Requirements Version 1.0*, **Upenn CIS Tech. Report MS-CIS-08-31.**