A Formally Verified SCUBA Dive Computer Based on Commodity Sensors

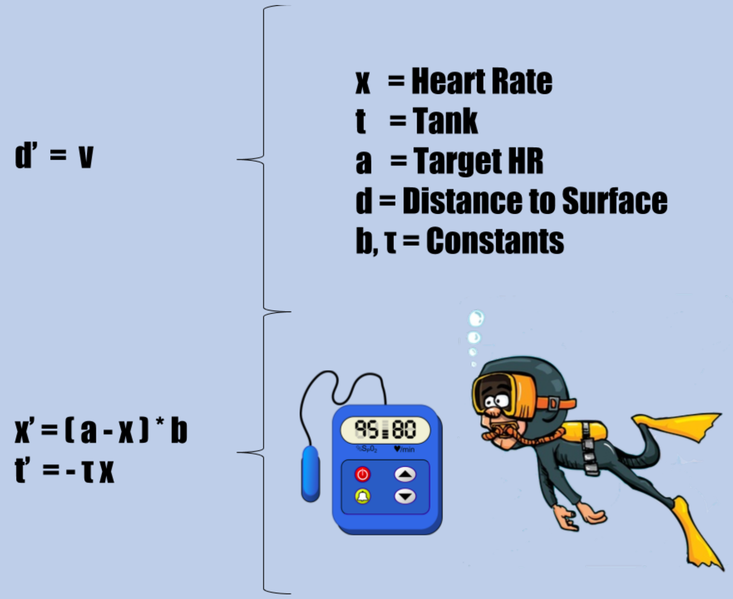
Viren Bajaj Karim Elmaroufi Nathan Fulton Andre Platzer
vbajaj@andrew.cmu.edu

Abstract

We present a model of a novel, formally verified **low-cost dive computer** which calculates oxygen consumption using the diver's heart rate in order to increase the time underwater and reduce the risk of decompression sickness. To monitor air supply, current cutting edge dive computers utilize a pressure gauge fixed on the tank that connects to a wrist watch through a wireless transmitter. Not only is this method very expensive, but it also adds a single point failure into a safety-critical system.
Our **novel approach toward safe diving** uses a commodity heart rate sensor and a mathematical model relating oxygen consumption and heart rate. Using these primitives, we calculate the volume of air remaining in the diver's tank. The safety of our SCUBA safety monitor is established using the highly trustworthy KeYmaera X theorem prover for Hybrid Systems.

Overview

Ensuring safe SCUBA diving requires reasoning about how the physical world will evolve in between two sensor measurements. We rely on **commodity heart-rate and depth sensors** together with a **mathematical model** relating heart rate to oxygen consumption.



Based on this model, we derive a control policy that allows the diver a range of movements while still ensuring that the diver can return to the surface without running out of oxygen. Using KeYmaera X, we developed the first formally verified SCUBA dive computer.

Model

$$\underbrace{t \geq 0 \land \cdots}_{\text{precondition}} \rightarrow [\{ctrl; \{\underbrace{ascend \cup stay \cup descend}_{\text{diver's behavioral model}}\}; plant\}^*] \underbrace{tank \geq 0}_{\text{postcondition}}$$

$$ctrl \equiv \{\texttt{NOP} \cup t_{worst} := t\}$$

$$ascend \equiv \{a := *; v := v_{asc}\}$$

$$stay \equiv \{?t_{worst} \geq \tau hr_{max}\epsilon + \tau hr_{max}\frac{-d}{v_{asc}}; a := *; v := 0\}$$

$$descend \equiv \{?t_{worst} \geq \tau * hr_{max} * \epsilon + \tau hr_{max}\frac{-d - v_{desc}\epsilon}{v_{asc}}; a := *; v := 0\}$$

$$plant \equiv c := 0; \{x' = b(a - x), t' = -\tau x, d' = v, c' = 1 \;\&\; d \geq 0 \land c \leq \epsilon\} \{t_{worst} := t_{worst} - \tau hr_{max} c\}$$

Our hybrid system program model is comprised of a controller, a behavioural model of the diver, a model of the physical world (*plant*), and a safety specification.

- The **controller** models the diver's ability to occasionally update the controller's approximation of the the tank volume (t_{worst}) to the actual value of the tank (t). The non-deterministic choice $\cup$ means that the system is safe even if the diver never updates the controller's over-approximation of the available oxygen.
- The **diver's behavioral model** splits the diver's kinematic decision space into three cases based on his vertical velocity, each of which has a different safety condition.
- The **plant** relates heart rate, oxygen consumption, and the diver's vertical movement.
- The **safety specification** is comprised of the initial conditions for which the system is safe and the post condition which ensures that the tank is never empty.

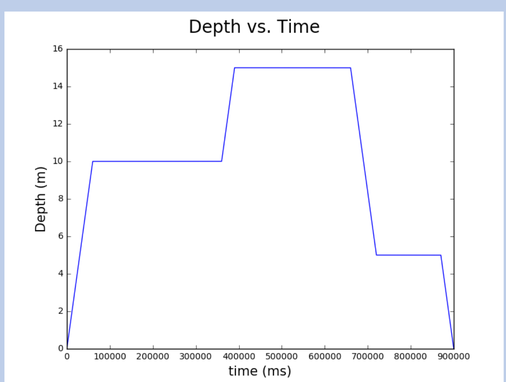
Our **computer-checked proof** of safety for this system makes use of advanced proof techniques, including *differential ghosts* to establish the invariant set $HR_{min} \leq x \leq HR_{max}$ and differential invariants to propagate safety constraints from the controller through the continuous dynamics.

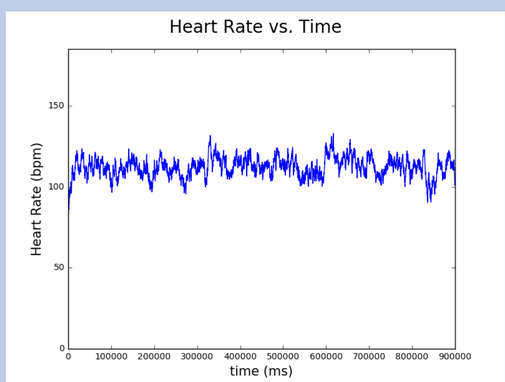
Simulations

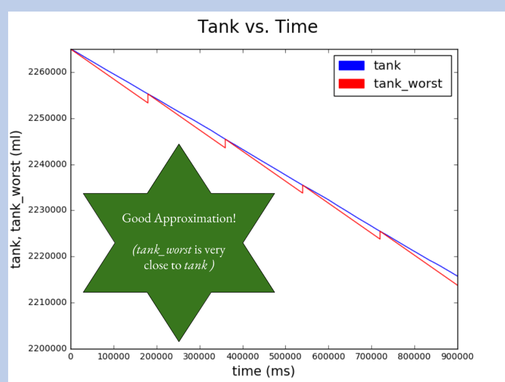
Subject: male, age 33
Height: 1.33m
Weight: 82 kg

VO_2^{max}: 49.7 ml min^{-1} kg^{-1}
HR_{max}: 185
HR_{min}: 40

b = 0.1968
τ=0.483 ml s^{-1}







Carnegie Mellon University
School of Computer Science