iCyPhy

Welcome and Introduction

Edward A. Lee

Professor of the Graduate School

iCyPhy Mini Workshop, Berkeley, Feb. 14, 2019

University of California at Berkeley

iCyPhy

Industrial Cyber-Physical Systems Center

Mission:

To make advanced software and networking technology usable in safety- and mission-critical industrial applications.

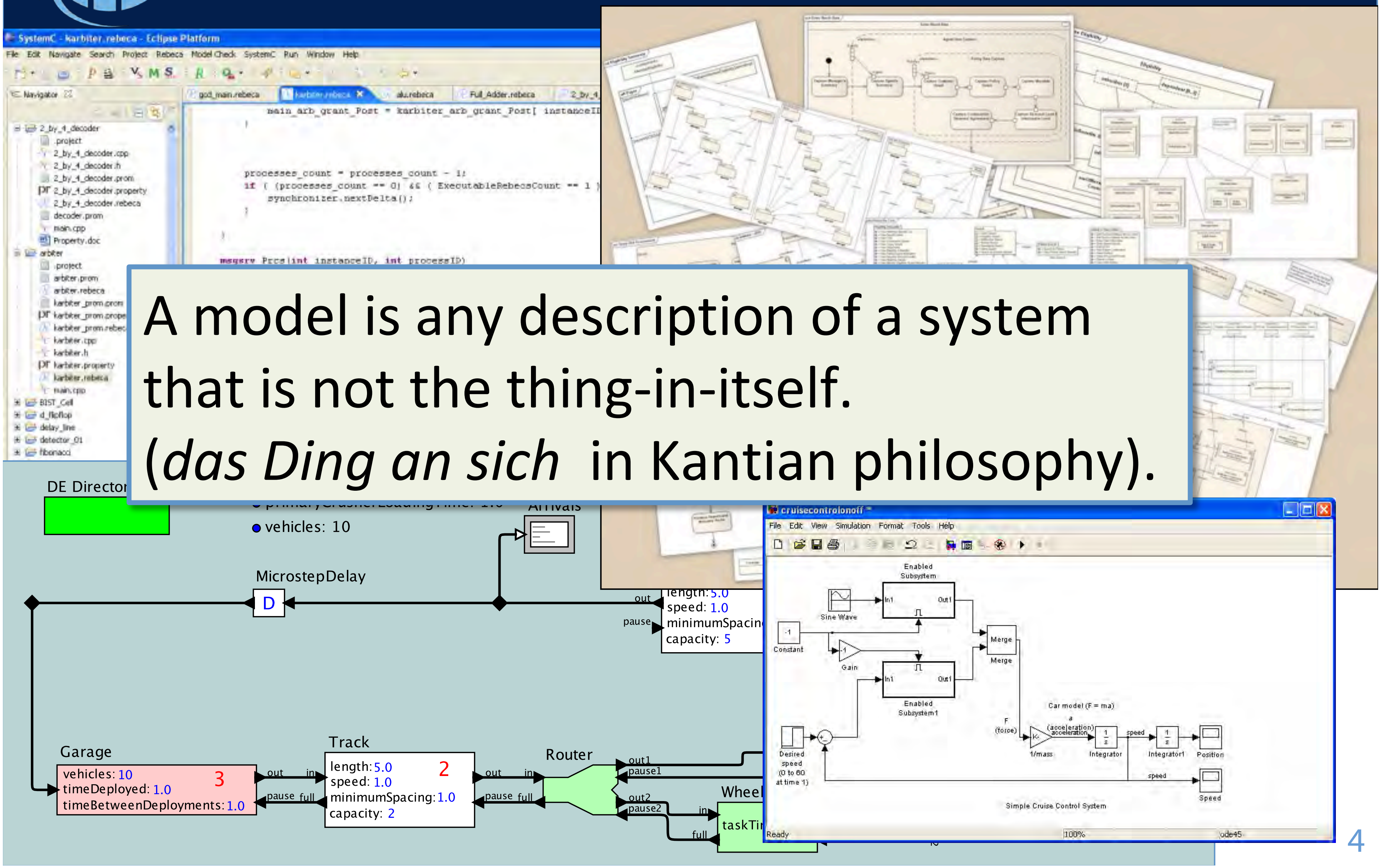



Prabal Dutta, Edward Lee, Alberto Sangionvanni-Vincetelli, Sanjit Seshia

Active Project Partners

- Avast
- Camozzi
- Denso
- Ford
- Siemens
- Toyota

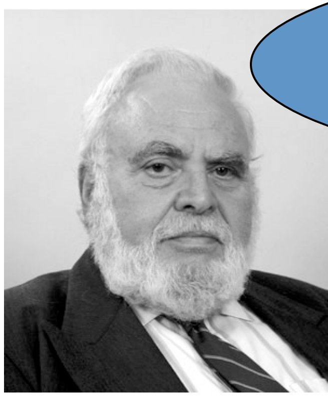
Focus on Models



A model is any description of a system that is not the thing-in-itself.
(*das Ding an sich* in Kantian philosophy).

Challenges

- Confusing the map and the territory
- Choosing a modeling paradigm
- Understanding the purpose of the model



You will never strike oil by drilling through the map!

Solomon Wolf Golomb

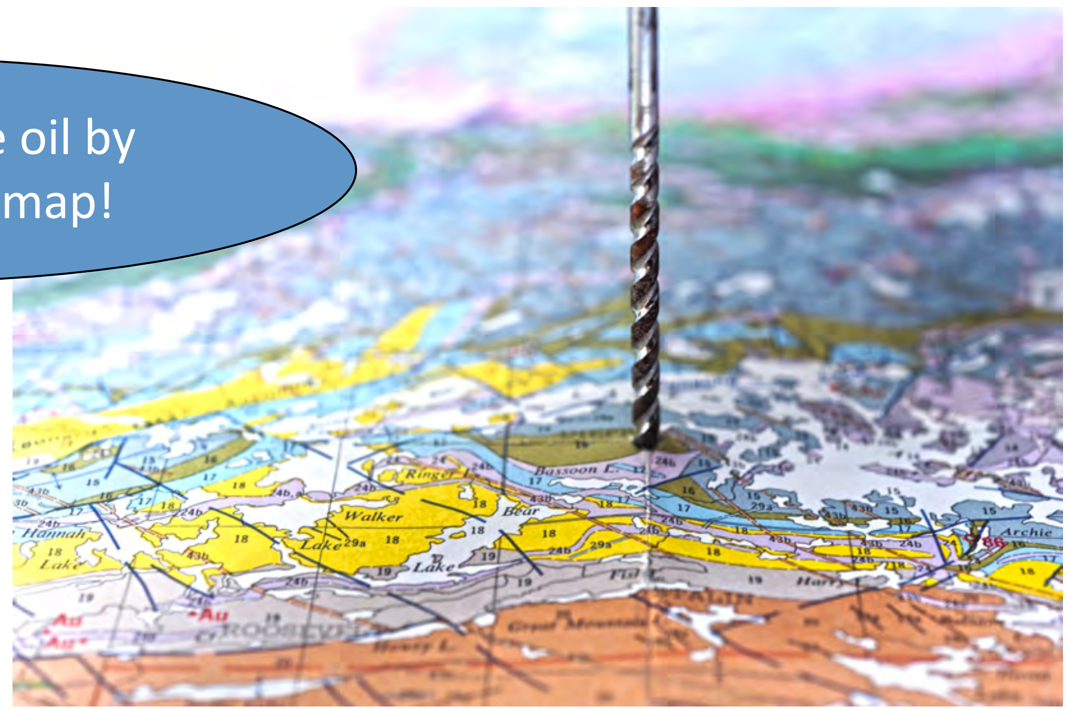


Photo by Rusi Mchedlishvili

Models vs. Reality

$$x(t) = x(0) + \int_0^t v(\tau)d\tau$$
$$v(t) = v(0) + \frac{1}{m}\int_0^t F(\tau)d\tau.$$

The model

The target (the thing being modeled).

In this example, the *modeling universe* is calculus and Newton's laws.

Faithfulness is how well the model and its target match

A Model

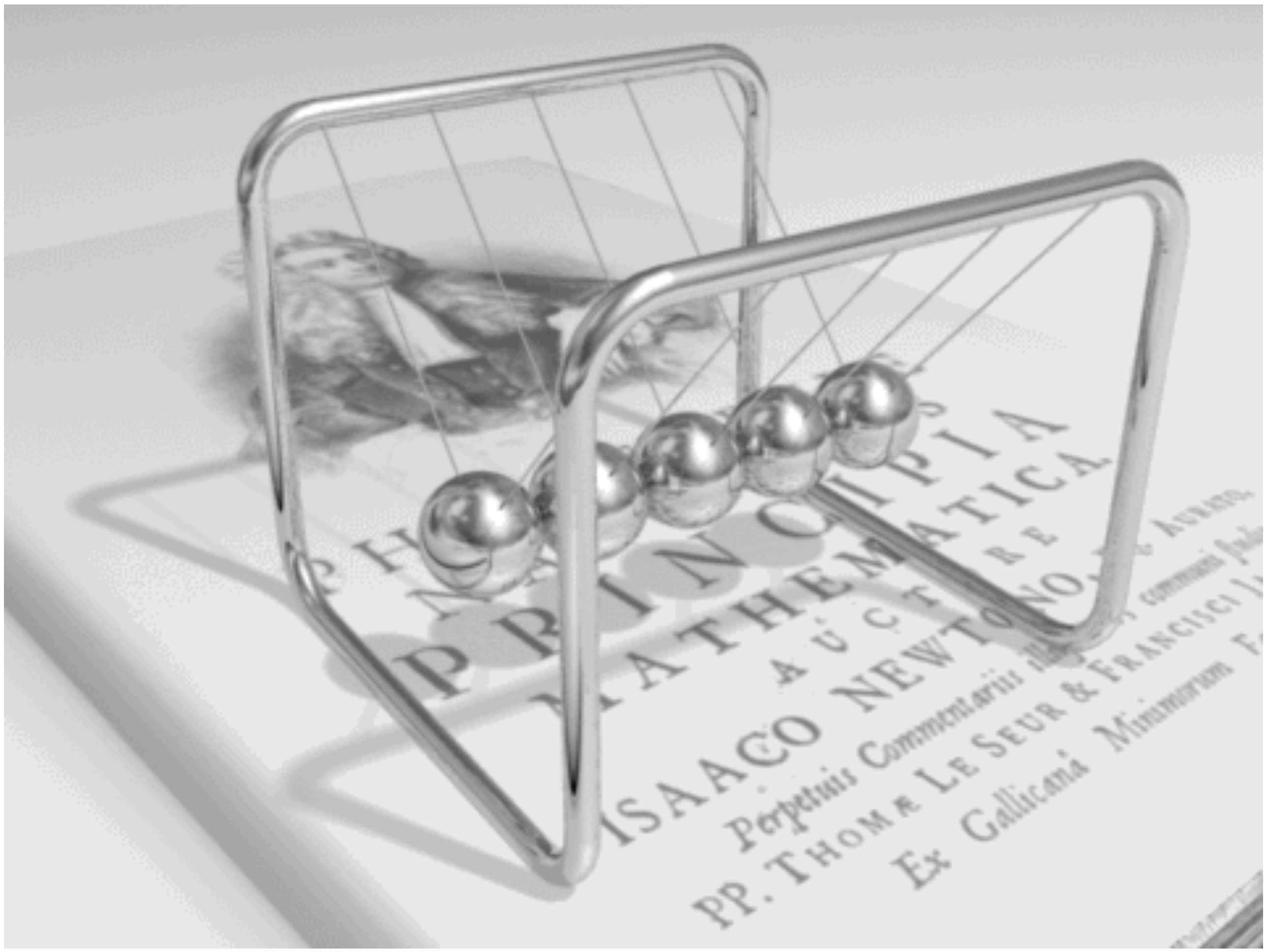
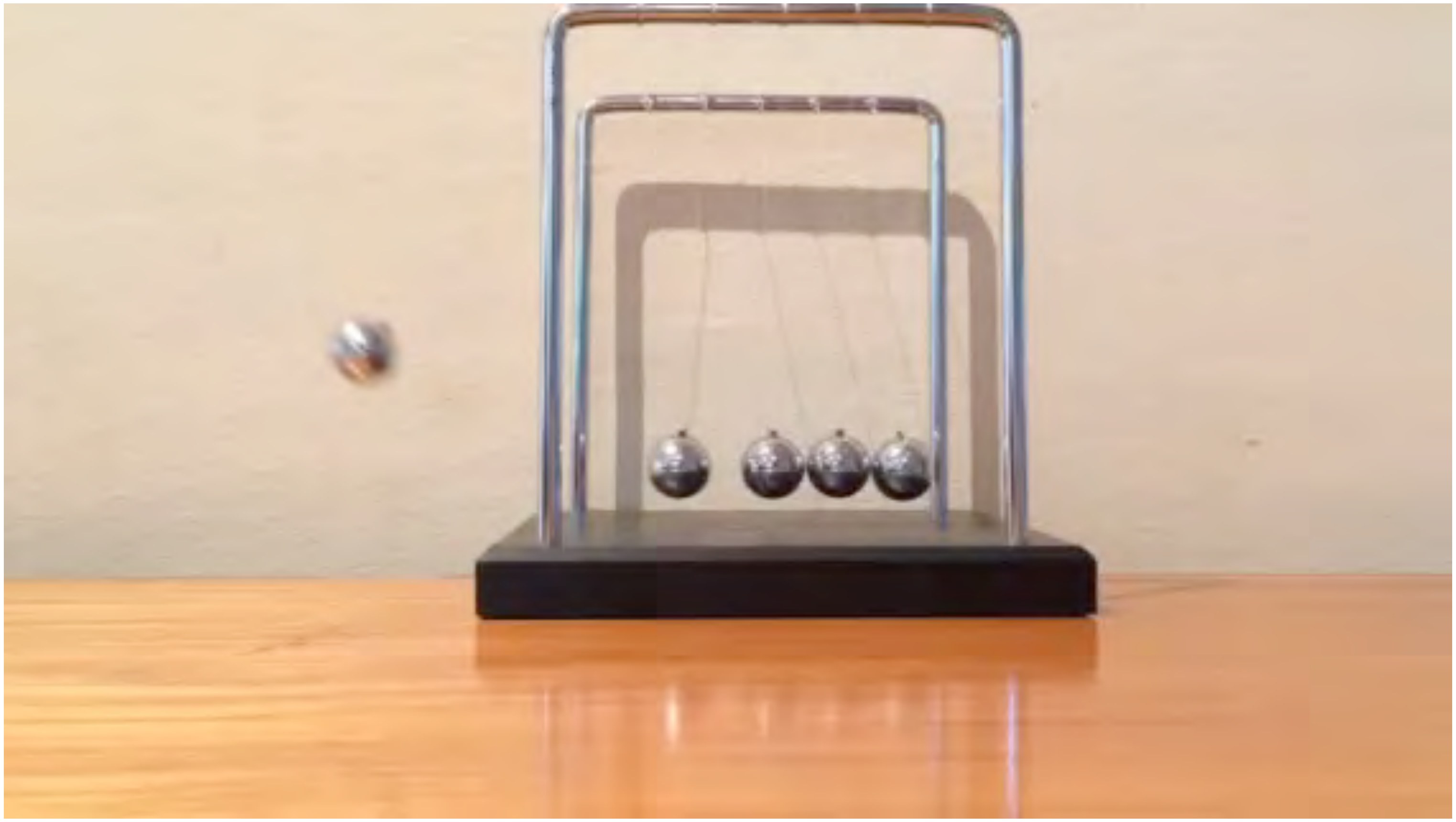


Image by Dominique Toussaint, GNU Free Documentation License, Version 1.2 or later.

A Physical Realization



The Value of Models

- In *science*, the value of a *model* lies in how well its behavior matches that of the physical system.

- In *engineering*, the value of the *physical system* lies in how well its behavior matches that of the model.

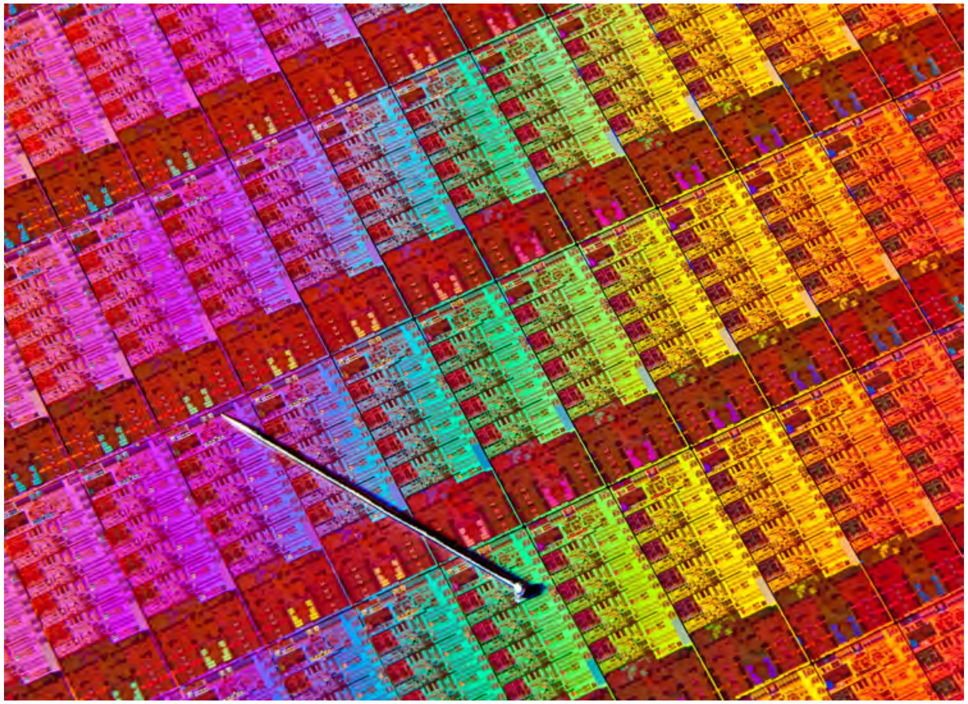
A scientist asks, "Can I make a model for this thing?"
An engineer asks, "Can I make a thing for this model?"

Model Faithfulness

- To a *scientist*, the model is flawed.
- To an *engineer*, the realization is flawed.

Engineering is more about making the thing match the model rather than the other way around.

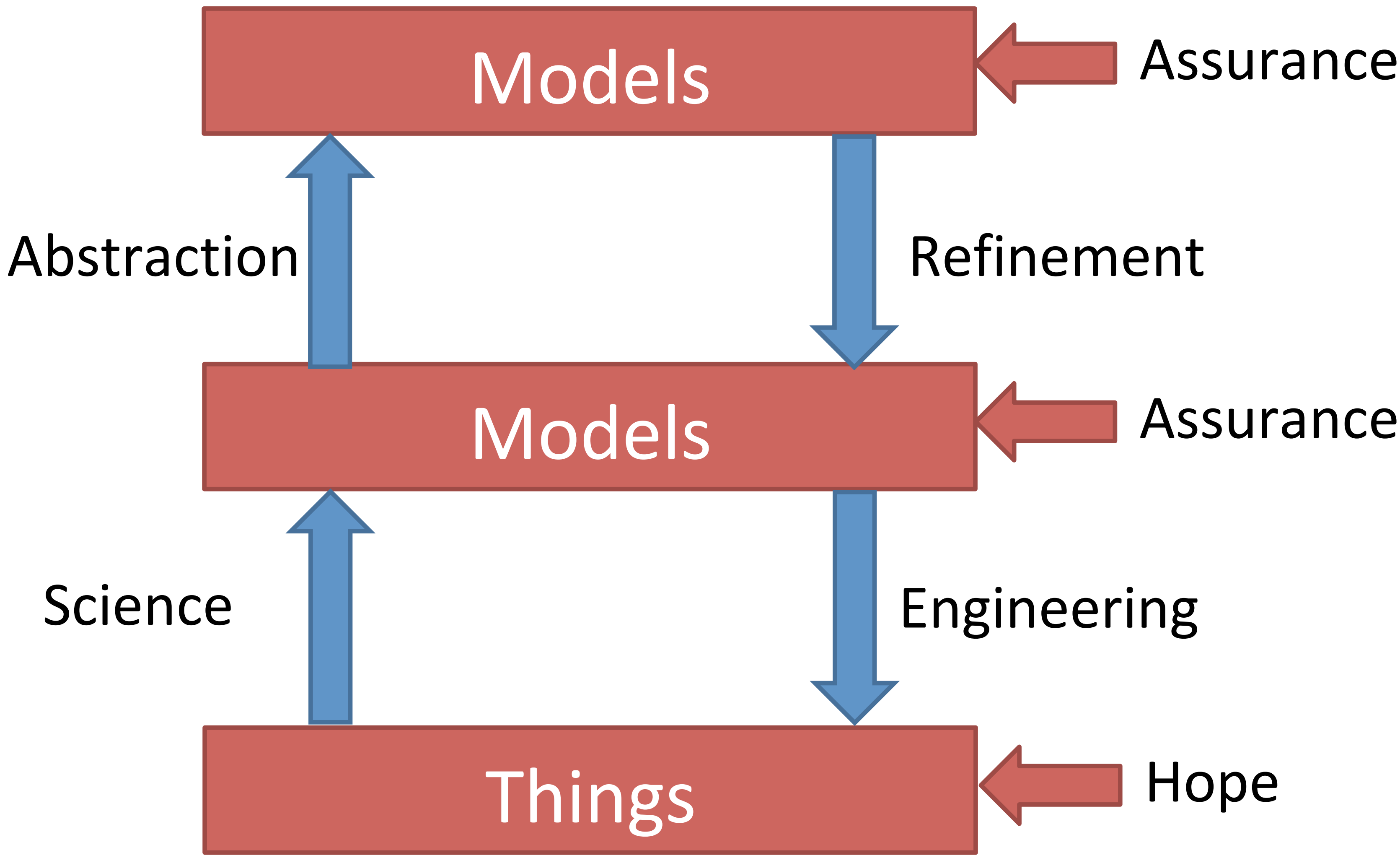
Consider Chip Design



Intel Haswell, each with 1.4 billion transistors

A piece of silicon that doesn't behave like the model is just beach sand.

Models and Models and Things



Useful Models and Useful Things

"Essentially, all models are wrong,
but some are useful."

Box, G. E. P. and N. R. Draper, 1987: *Empirical Model-Building and Response Surfaces*. Wiley Series in Probability and Statistics, Wiley.

"Essentially, all system implementations
are wrong, but some are useful."

Lee and Sirjani, "What good are models," FACS 2018.

Changing the Question

Is the question whether our models describe the thing in itself (faithfully)?

Or

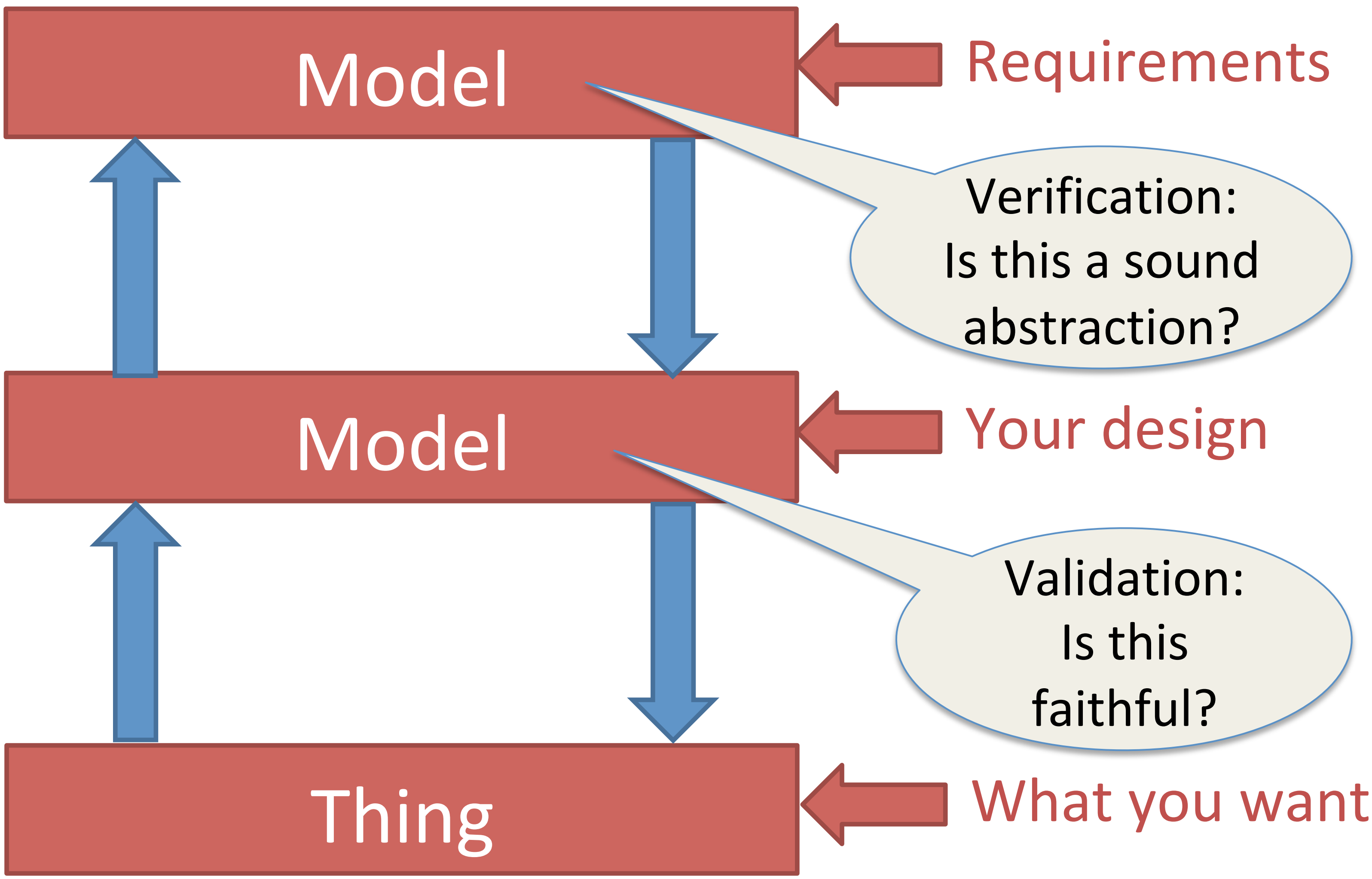
Is the question whether we can build a thing-in-itself where behavior matches that of our models (with high probability)?

Verification and Validation

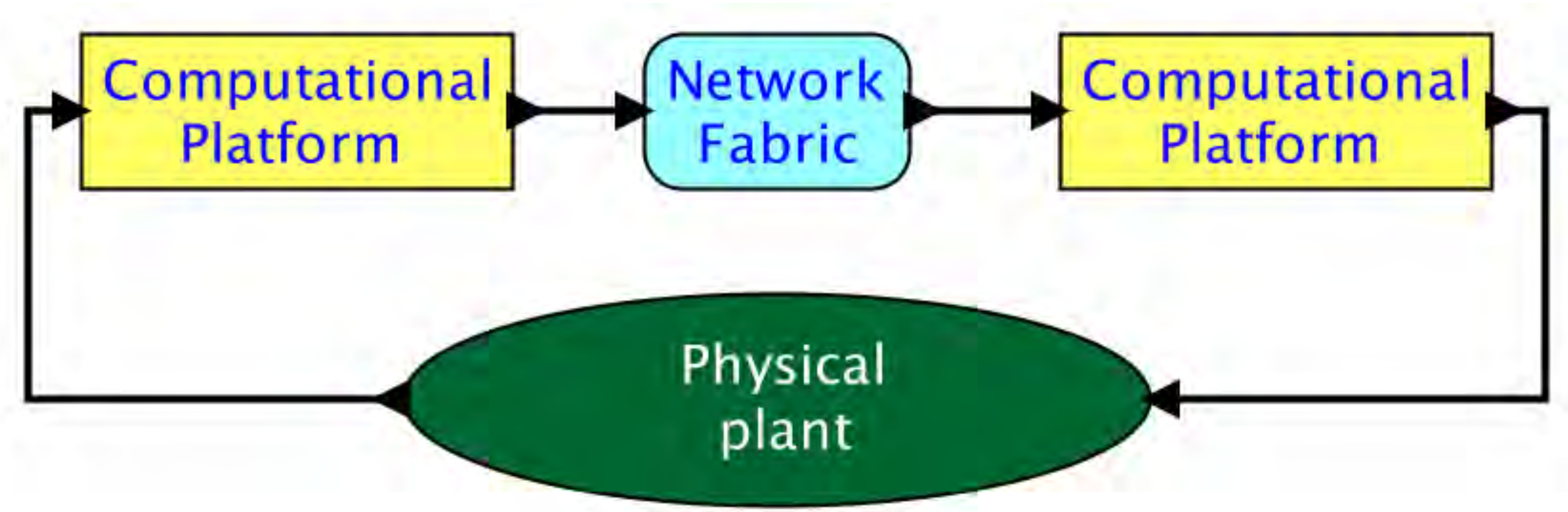
Per Boehm:

- Am I building the product right? (verification)
- Am I building the right product? (validation)

Verification and Validation



Cyber Physical Systems



What kinds of models should we use?

Software as a Model

Physical System

Model

```java
/** Reset the output receivers, which are the inside receivers of
 *  the output ports of the container.
 *  @exception IllegalActionException If getting the receivers fails.
 */
private void _resetOutputReceivers() throws IllegalActionException {
    List<IOPort> outputs = ((Actor) getContainer()).outputPortList();
    for (IOPort output : outputs) {
        if (_debugging) {
            _debug("Resetting inside receivers of output port: "
                    + output.getName());
        }
        Receiver[][] receivers = output.getInsideReceivers();
        if (receivers != null) {
            for (int i = 0; i < receivers.length; i++) {
                if (receivers[i] != null) {
                    for (int j = 0; j < receivers[i].length; j++) {
                        if (receivers[i][j] instanceof FSMReceiver) {
                            receivers[i][j].reset();
                        }
                    }
                }
            }
        }
    }
}
```

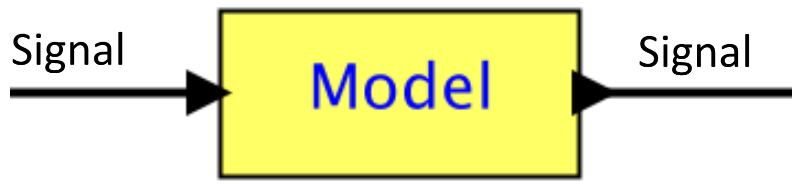
Single-threaded imperative programs
are deterministic models

Physics as a Model

Physical System

Image: Wikimedia Commons

Model

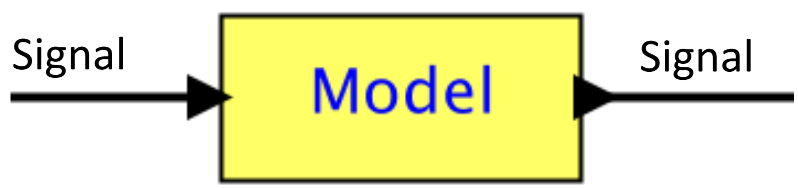


$$\dot{\mathbf{x}}(t) = \dot{\mathbf{x}}(0) + \frac{1}{M}\int_0^t \mathbf{F}(\tau)d\tau$$

Differential Equations
are deterministic models

A major problem for CPS: combinations of deterministic models are nondeterministic

```
void initTimer(void) {
    SysTickPeriodSet(SysCtlClockGet() / 1000);
    SysTickEnable();
    SysTickIntEnable();
}
volatile uint timer_count = 0;
void ISR(void) {
    if(timer_count != 0) {
        timer_count--;
    }
}
int main(void) {
    SysTickIntRegister(&ISR);
    .. // other init
    timer_count = 2000;
    initTimer();
    while(timer_count != 0) {
        ... code to run for 2 seconds
    }
    ... // other code
}
```



$$\dot{\mathbf{x}}(t) = \dot{\mathbf{x}}(0) + \frac{1}{M}\int_{0}^{t} \mathbf{F}(\tau)d\tau$$

 Image: Wikimedia Commons

Our Strategy

Find engineering models for which we can:

- build faithful realizations,
- verify properties we care about, and
- design interesting and useful systems.