Principles of Modeling for Cyber-Physical Systems

Fall 2018
CS 6501-003 / SYS 6581-004/600

Madhur Behl
Computer Science
Systems and Information Engineering
Meet your instructor

Madhur Behl

Physicist at

Cyber-Physicist by profession

Assistant Professor
Computer Science,
Systems and Information Engineering.

PhD, University of Pennsylvania (2015)
Co-Founder @ Flexergy AI
What do I do..

Modeling, simulation, control, optimization, and implementation of Cyber-Physical System

Data Predictive Control:
Interfacing machine learning suitable for predictive control.

DeepExplainations:
Answering open-ended queries using procedural generation and interpretable models.

DeepRacing AI:
Algorithms for operating autonomous cars at the limits of their control

Internet of things
This lecture

• Course logistics (5-7 mins)
• Course introduction (the interesting stuff!)

Principles of modeling for CPS – Fall 2019
Madhur Behl - madhur.behl@virginia.edu
Course Logistics

- **Timings:** Tue & Thu 2:00pm – 3:15pm,
- **Location:** Olsson Hall 018

- **Course website:** [https://linklab-uva.github.io/modeling_cps/](https://linklab-uva.github.io/modeling_cps/)
  - All lectures notes/slides/assignments/videos will be posted on this website.


- **Prerequisites (must have):**
  - Some familiarity with Matlab / Simulink.
  - Some programming experience, Python is a plus.
  - Mathematical maturity (differential equations, matrix operations, some calculus, probability distributions)

- **Prerequisites (good to have):**
  - Machine learning
  - Temporal logic
  - Model predictive control
Teaching Assistants

Siavash Yousefi Jordehi

sy3fw@virginia.edu
Systems Engineering, PhD

Jiechao Gao

jg5ycn@virginia.edu
Computer Science, PhD

Office Hours: TBA
Grading

• No midterm, No final exam.

• The course has three modules (more on this later). Each module is equally weighted.
  • Energy CPS, Medical CPS, and Automotive CPS

• ~4 worksheets (posted on UVACollab/Website) in each module, comprising of:
  • Problem sets
  • Coding/implementation assignments

• 2 late homework submissions permitted – No questions asked.
  • Should not be more than 1 day late. 25% grade lost for each additional late day.

• Abide by the UVA honor system. Absolutely no code/solution sharing!
Office Hours

• **Timings:** Monday 2-3pm, or by appointment.

• **Location:** Link Lab Room 265 [Olsson Hall 2\textsuperscript{nd} floor]

• Available by appointment outside of the listed hours:
  • To discuss course assignments or lectures.
  • Research opportunities.

• Live streamed office hours will be held for online CGEP students.
Your responsibilities.

- Attend the lectures (in-person for on-grounds students)
- Check Piazza and the Course website for announcements, and assignments.
- Ask questions!
  - Ask, disagree, debate..
what is this course about?

Principles of Modeling for Cyber-Physical Systems

Lets break it down..

1. What are Cyber-Physical Systems?
2. What do you really mean by modeling?
3. What principles am I going to learn about?
Cyber-Physical Systems

Deeply integrating

computation, communication, and control

into physical systems

Physical = some tangible, physical device or system + environment
Cyber = computational + communicational
Application domains: Transportation

Faster, safer, more energy-efficient air travel

Improved use of airspace

Autonomous unmanned drones
How the MCAS (Maneuvering Characteristics Augmentation System) works on the 737 MAX

1. The angle-of-attack sensor aligns itself with oncoming airflow. The angle of attack is the angle between the wing and the airflow.

2. Data from the sensor is sent to the flight computer. If the angle rises too high, suggesting an approaching stall ...

3. MCAS automatically swivels the horizontal tail to lift the plane’s tail while moving the nose down. ... the MCAS activates.

In the Lion Air crash, the angle-of-attack sensor fed false information to the flight computer.

Sources: Boeing, FAA, Indonesia National Transportation Safety Committee, Leeham.net, and The Air Current

Reporting by DOMINIC GATES, Graphic by MARK NOWLIN / THE SEATTLE TIMES
Unique requirements for safeguarding aircraft

Cyber-physical systems are ones that integrate physical components through computation and networking, and they present unique challenges and opportunities for cyber defense.

Wherever there are computers, there is the potential for adversaries to attempt to subvert them for their own purposes.

First the challenge: cyber-physical systems like aircraft are typically more resource constrained—including in connectivity—than desktop and enterprise systems (and even mobile systems). This means that desktop and enterprise security solutions relying on spare computing power, storage and always-on high-bandwidth networking, generally cannot be used on cyber-physical systems. This complicates the problem for cyber defense.

But here's the opportunity: cyber-physical systems are generally designed for a specific purpose and to interact with the physical world. In other words, their behaviors tend to be designed to achieve a physical result.
Application domains: Transportation

Safety, security, and control of autonomous cars

- Connected vehicles.
- Autonomous fleets/ride sharing.
- Traffic management
Application domains: Energy

- Smart buildings.
- Energy-efficient operation.
- Smart homes.
- EV charging/solar rooftops
- Reliable and resilient electricity grid.
- Micro grids.
Application domains: Healthcare + Biomedical

- Electronic patient record management.
- In home healthcare delivery.

Health and well being monitoring devices.

Safety, and security of medical devices and health management systems.
Application domains: Critical Infrastructure

- Water & waste management.
- Storm-water/flood control.
- Structural health monitoring
- Utility infrastructure- Gas, Electricity, Steam.
Application domains: ... and many more

Agriculture
Manufacturing
Industrial Control
Characteristics of CPS

- Pervasive computation, sensing and control
- Networked at multi- and extreme scales
- Dynamically reorganizing/reconfiguring
- High degrees of automation

- Dependable operation with potential requirements for high assurance of reliability, safety, security and usability
- With / without human in-the-loop
- Conventional and unconventional substrates / platforms
Closing the loop

Cyber

Physical

Controller

Sensing

Actuation

Plant/System
Human in the loop

[Diagram showing the human in the loop concept in a closed control system with labelled parts: Sensing, Controller, Plant/System, and Actuation.]
Cyber-Physical Systems

Deeply integrating

computation, communication, control, and humans

into physical systems

Physical = some tangible, physical device or system + environment
Cyber = computational + communicational
Cyber-Physical Systems - Goals

Transform how we interact with the physical world

Fusion of physical and computational sciences

Produce significant impact on society
Why is CPS hard?

Computing

Control

Systems

Crosses Interdisciplinary Boundaries
Why is CPS hard?

- Disciplinary boundaries need to be realigned
- New **fundamentals** need to be created
- New **technologies and tools** need to be developed
- Education need to be restructured
Why is CPS hard?

- Disciplinary boundaries need to be realigned
- New **fundamentals** need to be created
- New **technologies and tools** need to be developed
- **Education needs to be restructured**

Hmmm, I wonder if there is a course which is trying to achieve this?
what is this course about?

Principles of **Modeling** for Cyber-Physical Systems

Lets break it down..

1. What are Cyber-Physical Systems?
2. What do you really mean by modeling?
3. What principles am I going to learn about?
Modeling types: Physical modeling
Modeling types: Functional/compositional modeling

Do you know of any tools for functional modeling?
Modeling types: Mathematical modeling

\[
\begin{align*}
\dot{v}_x &= \frac{1}{m} \left[ (F_{xL}^{fL} + F_{xR}^{fR}) \cos \delta - (F_{yL}^{fL} + F_{yR}^{fR}) \sin \delta + (F_{xL}^{rL} + F_{xR}^{rR}) + \phi v_y \right], \\
\dot{v}_y &= \frac{1}{m} \left[ (F_{yL}^{fL} + F_{yR}^{fR}) \cos \delta + (F_{xL}^{fL} + F_{xR}^{fR}) \sin \delta + (F_{yL}^{rL} + F_{yR}^{rR}) - \phi v_x \right], \\
\dot{\phi} &= \frac{1}{I_p} \left[ L_f (F_{xL}^{fL} + F_{xR}^{fR}) \sin \delta + L_f (F_{yL}^{fL} + F_{yR}^{fR}) \cos \delta - L_r (F_{yL}^{rL} + F_{yR}^{rR}) \right] \\
&\quad + \frac{L_w}{2} (F_{xL}^{fL} - F_{xR}^{fL}) \cos \delta + \frac{L_w}{2} (F_{xL}^{fR} - F_{xR}^{fR}) \sin \delta + \frac{L_w}{2} (F_{yL}^{fL} - F_{yR}^{fL}) \cos \delta + \frac{L_w}{2} (F_{yL}^{fR} - F_{yR}^{fR}) \sin \delta.
\end{align*}
\]
Modeling types: Computational modeling
A word about mathematical models

Observational errors → Physical System Reality → Observations → Mathematical models → Modeling errors → Computational/Simulation models → Discretization errors → Control & implementation → Verification

Validation
“Essentially all models are wrong, but some are useful”

- George E.P. Box (statistician)

....this course is about building useful models.
This course: Three CPS domains

Energy CPS

Medical CPS

Automotive CPS
Principles of modeling for CPS – Fall 2019

Madhur Behl – madhur.behl@virginia.edu
Energy CPS

Medical CPS

Automotive CPS

EnergyPlus

UPPAAL

Simulink

TensorFlow

Python
Energy CPS Module
2014 Officially Hottest Year on Record

2015 Is Officially the Hottest Year

July Was the Hottest Month in Recorded History

After a record-breaking heat wave in Europe and the Arctic, last month edged out July 2016 on record for the U.S.

2018 Was the 4th Warmest Year on Record, Berkeley Group Announces
Price Volatility: Summer peak

Nominal price: $25/MWh  
Peak Price: $800/MWh

32x!
“All kilowatts are not created equally”
Heat wave results in highest U.S. electricity demand since 2017

Hourly electricity demand in the Lower 48 states (Jul 7-Jul 27, 2019)

Source: U.S. Energy Information Administration, *U.S. Electric System Operating Data*
Price Volatility: Winter peak

Nominal price: $31.21/MWh
Peak Price: $2,680.21/MWh

24th, January 2014
Price volatility is the new normal

PJM (ISO) Locational Marginal Prices (LMPs) example
At large scales: University Campus

- 72 MW Peak (UCAP)
- 187 Buildings
- 300,000 SCADA Tags
- 4 Million Gallons of chilled water (@42F)
Economic incentives for model based control

~$28M Annual Electricity Bill

In 2011

Peak > UCAP

30 min

$720,000 Penalty for 30 minutes
Why focus on Buildings?

- 40% Portion of global energy use
- 70% Portion of electricity consumption in the United States
- 1/3 Portion of global total CO₂ emissions
Model-Based control for buildings

**Traditional rule-based building control**

- Sequence of operations or planned steps.
- Pre-defined rules set by building engineers.
- Purely reactive.
- Equipment-level controllers (PID) ensure reference tracking.

**Model-based building control**

- Model how the building will respond to disturbances (weather, occupants etc.)
- Predictive
- Control design:
  - Energy-efficiency
  - Demand flexibility
  - Fault handling
- Okay to use equipment level PID control

Took 23 min yesterday

Took 42 min today (but price increased!)

**Model Predictive Control (MPC)**
The control problem in buildings

Integrated control of:

• Heating
• Cooling
• Ventilation
• Lighting
• Blinds
State-space ‘RC’ thermal modeling

\[ C_{co} \dot{T}_{co}(t) = U_{co} (T_a(t) - T_{co}(t)) + U_{cw} (T_{ci}(t) - T_{co}(t)) + Q_{sol,c}(t) \]
\[ C_{ci} \dot{T}_{ci}(t) = U_{cw} (T_{co}(t) - T_{ci}(t)) + U_{ci} (T_z(t) - T_{ci}(t)) + Q_{rad,c}(t) \]
Whole building energy simulation


Generating input-output data

Modeling a building in MATLAB
Non-linear parameter estimation and model validation

Model Accuracy for Training data
RMSE: 0.062 °C
R²: 0.983

Baseline

Model Accuracy for Test Data
RMSE: 0.091 °C
R²: 0.948
Predictive control
Medical CPS Module
Software related vehicle recalls

Principles of modeling for CPS – Fall 2019
Madhur Behl - madhur.behl@virginia.edu
Implantable devices recall

- Over 600,000 cardiac medical devices recalled from 1990-2000
  - 40% of which were due to software issues

- 2008-12: **15% of all** the medical device recalls due to software

Implantable Pacemaker

Implantable Cardioverter-Defibrillator (ICD)
The Heart

- Muscle contraction triggered by electrical signals
Bradycardia

- Slow generation and conduction of electrical signals
- Slow heart rate
- Symptom: fainting, dizziness
- Could lead to heart attack
Implantable Pacemaker

- No leads in heart chambers
• Two leads in heart chambers
• Deliver electrical signals when heart rate is low
**Implantable Pacemaker**

- Two leads in heart chambers
- Deliver electrical signals when heart rate is low
- Device malfunction may result in *injury or death*
- Flawed devices are recalled
CHALLENGES

Pacemaker
Autonomous device with minimum human interaction
Limited diagnostic/therapy capability
Its safety must be evaluated within its environment

The physical plant:
Complex dynamics of the heart
Interaction between the heart and the body
Domain knowledge
Personalized Virtual Hearts Could Improve Cardiac Surgery

Digital replicas of patients' hearts can identify hidden, irregular heart tissue for surgeons to destroy

By Megan Scudellari
HEART MODELING

Principles of modeling for CPS – Fall 2019

Madhur Behl - madhur.behl@virginia.edu
CLOSED-LOOP HEART MODELING
Cellular Level

Node Automaton

• Divide refractory period into time periods
• Model refractory properties as timers using timed automata.
• These time periods can be measured during EP study
Cellular Level

Node Automaton

- RRP ends
- REST
- Self-depolarized or activated
- ERP ends
- RRP
- ERP
- Activated*

* With changes in ERP and conduction speed of paths connecting to the node

Madhur Behl - madhur.behl@virginia.edu
The UPPAAL model of the closed-loop system
Model checking – Counter example guided.

Safety property

Ventricular rate should not be equal or above the upper rate limit for more than 30 beats

$A[] \neg \text{monitor.err}$
Automotive CPS Module
Localization and Mapping
Where am I?

Scene Understanding
Where/who/what/why of everyone/everything else?

Trajectory Planning and Control
Where should I go next?
How do I steer and accelerate?

Human Interaction
How do I convey my intent to the passenger and everyone else?
Localization and Mapping
Where am I?

Scene Understanding
Where/who/what/why of everyone/everything else?

Trajectory Planning and Control
Where should I go next?
How do I steer and accelerate?

Human Interaction
How do I convey my intent to the passenger and everyone else?
Localization and Mapping
Where am I?

Scene Understanding
Where/who/what/why of everyone/everything else?

Trajectory Planning and Control
Where should I go next?
How do I steer and accelerate?

Human Interaction
How do I convey my intent to the passenger and everyone else?
End-to-End Deep Learning for Self Driving Cars

Center camera → CNN → Steering command → Drive-by-wire interface

Video credit: DeepTesla

Principles of modeling for CPS - Fall 2019
Madhur Behl - madhurbehl@virginia.edu
Machine intelligence is largely about training data.
When’s a pedestrian not a pedestrian? When it’s a decal.
One car ? or Multiple cars ?
Ramen Noodle place or Do Not Enter Sign?
There is a bus right next to you!!
Autonomous Driving: End-to-End
Autonomous Driving: End-to-End

End to End Learning for Self-Driving Cars

Mariusz Bojarski  
NVIDIA Corporation  
Holmdel, NJ 07735

Davide Del Testa  
NVIDIA Corporation  
Holmdel, NJ 07735

Daniel Dworakowski  
NVIDIA Corporation  
Holmdel, NJ 07735

Bernhard Firner  
NVIDIA Corporation  
Holmdel, NJ 07735

Beat Flepp  
NVIDIA Corporation  
Holmdel, NJ 07735

Prasoon Goyal  
NVIDIA Corporation  
Holmdel, NJ 07735

Lawrence D. Jackel  
NVIDIA Corporation  
Holmdel, NJ 07735

Mathew Monfort  
NVIDIA Corporation  
Holmdel, NJ 07735

Urs Muller  
NVIDIA Corporation  
Holmdel, NJ 07735

Jiakai Zhang  
NVIDIA Corporation  
Holmdel, NJ 07735

Xin Zhang  
NVIDIA Corporation  
Holmdel, NJ 07735

Jake Zhao  
NVIDIA Corporation  
Holmdel, NJ 07735

Karol Zieba  
NVIDIA Corporation  
Holmdel, NJ 07735
Autonomous Driving: End-to-End
F1/10 FPV Driving
Predicted: -0.04  Ground Truth: -0.00
what is this course about?

Principles of Modeling for Cyber-Physical Systems

Lets break it down..

1. What are Cyber-Physical Systems?
2. What do you really mean by modeling?
3. What principles am I going to learn about?
This course: Modeling principles

- Modeling for predictive control.
- Parameter estimation.
  - Linear and non-linear
- Model checking
- Model validation
- Model selection
  - Model abstraction/reduced order modeling
- End-to-end learning
This course: Learning objectives

Domain Expert (Physical System)

Modeling principles

Tools & implementation
This course: Learning objectives

The future belongs to those who learn more skills and combine them in creative ways.
This course: **Becoming a Cyber-Physicist**

- Energy CPS
- Automotive CPS
- State-Space Modeling
- Model checking
- Parameter estimation
- First principles modeling
- Data-driven modeling
- Timed automata
- UPPAAL
- EnergyPlus

**Principles of modeling for CPS – Fall 2019**

Madhur Behl - madhur.behl@virginia.edu
Next lecture:

• How to predict the future..
  • State-space modeling using first principles.
  • Mechanical, electrical, thermal systems
  • ODEs and elements of white box modeling