Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste

II Semestre 2020

Lecture 1: Introduction and Course Logistic

Course Logistics

Timing

- Laura: Wed & Fri 11-13:00, (sometimes Mon), aula 5A
- Some seminars

Course Website

Moodle

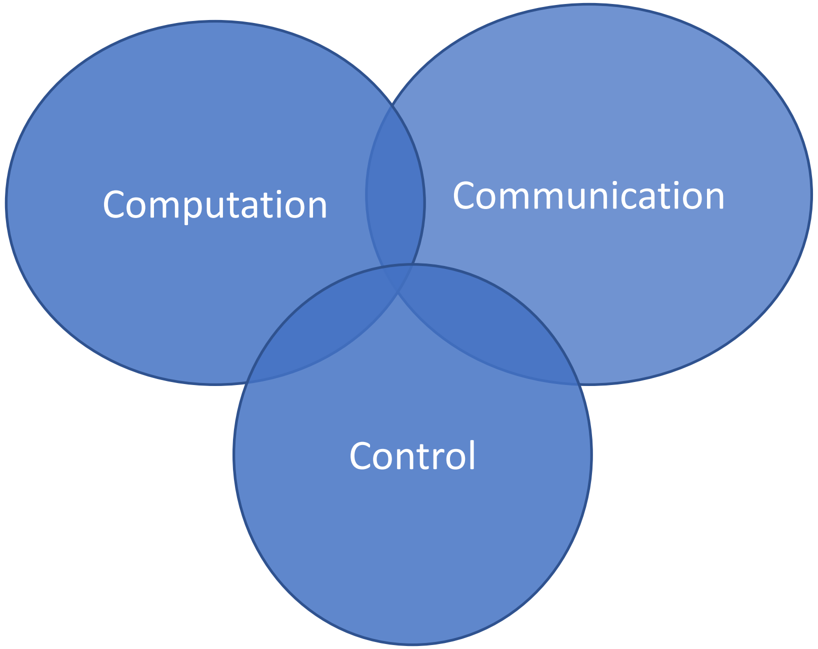
Teams

What is a Cyber-Physical System?

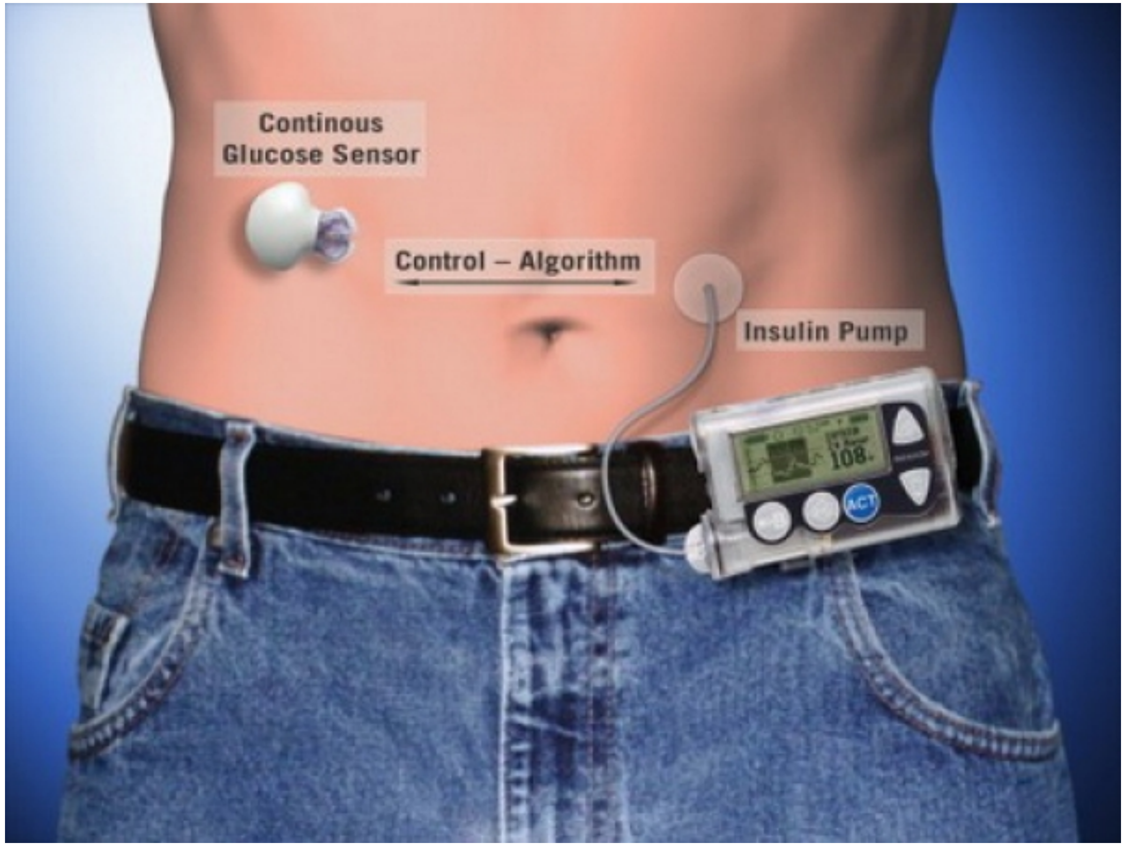
A CPS is a **mechanism** that is controlled or monitored by **computer-based algorithms**, tightly integrated with the Internet and its users.

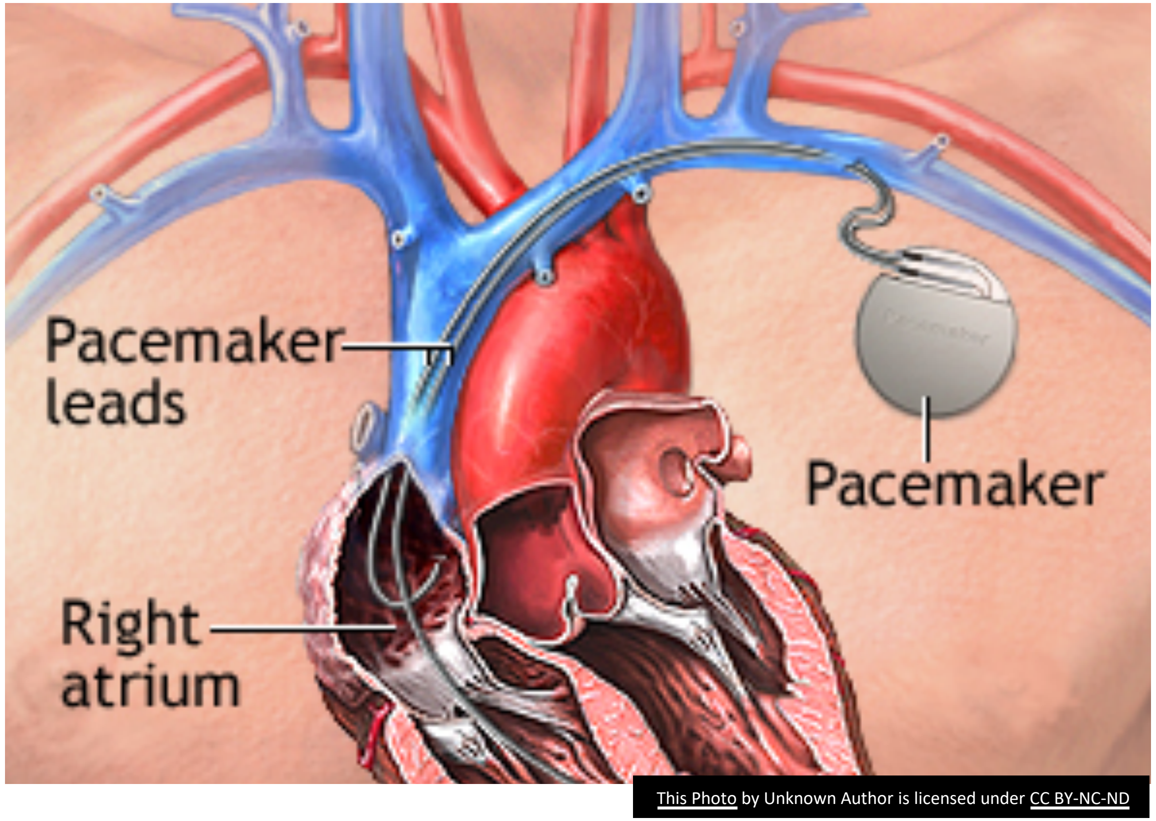
Physical = physical device or system + environment

Cyber = computational + communicational



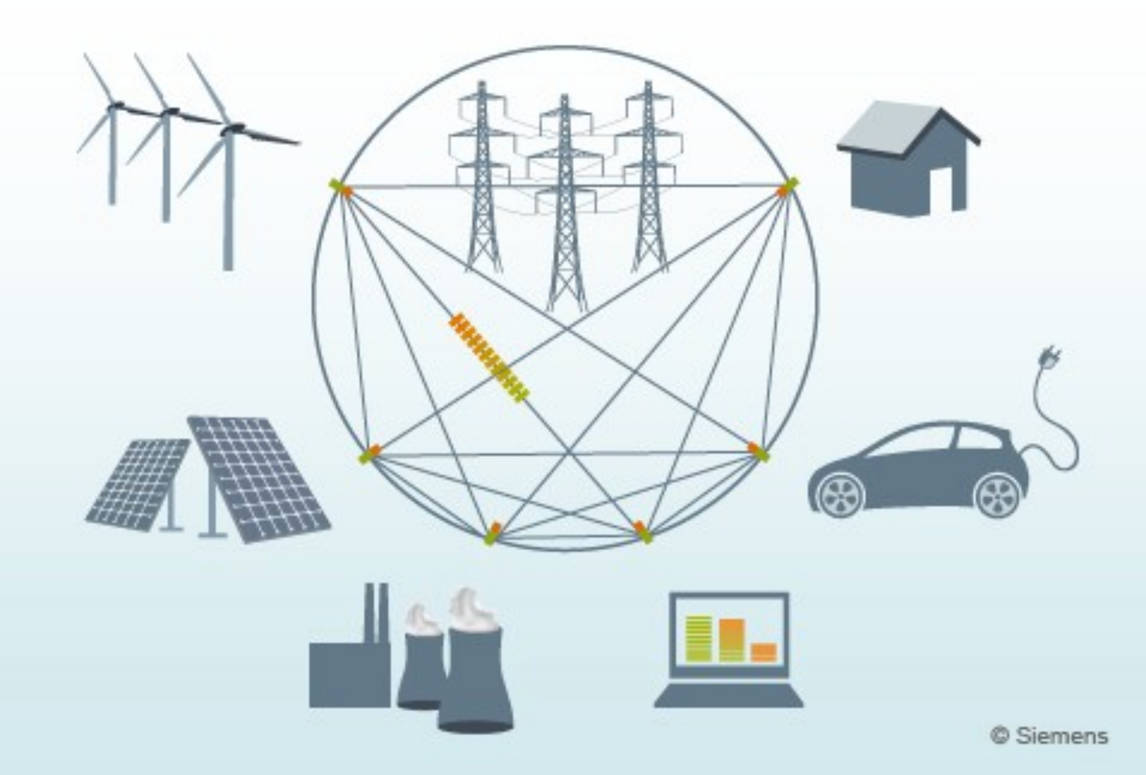
Medical Device

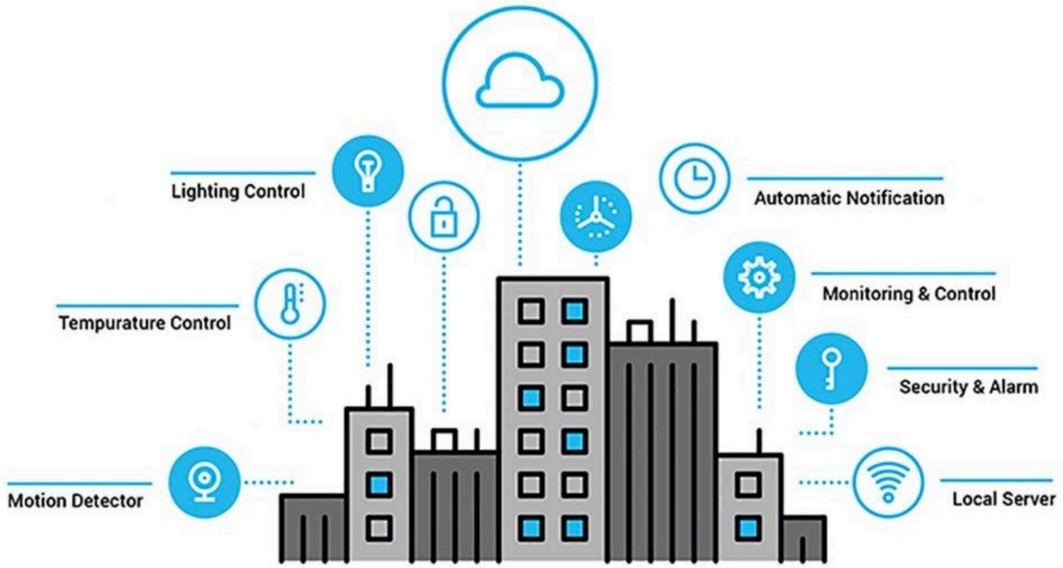




Transportation

Energy


© Siemens


Lighting Control
Automatic Notification
Monitoring & Control
Tempurature Control
Security & Alarm
Motion Detector
Local Server

And many other applications…

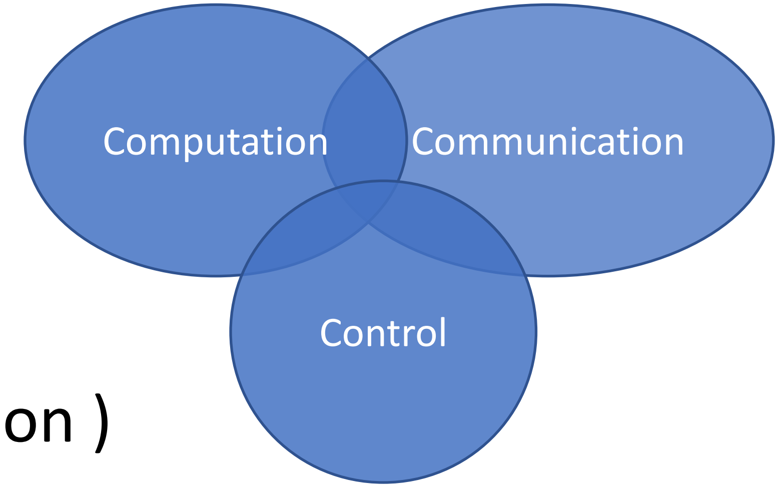
- Robotics
- Critical Infrastructures
- Industrial Control
- Manufactering
- Agricolture

What is a Cyber-Physical System?

A CPS is a **mechanism** that is controlled or monitored by **computer-based algorithms**, tightly integrated with the Internet and its users.

Physical = physical device or system + environment

Cyber = computational + communicational



Coined in 2006 by Helen Gill (National Science Foundation)

The important part in CPS is the conjunction/intersection between the computing part and physical dynamics

What is a Cyber-Physical System?

In cyber-physical systems, physical and software components are **deeply intertwined**, each operating on **different spatial and temporal scale**, exhibiting **multiple and distinct behavioral modalities**, and interacting with each **other in a lot of ways** that change with context.

CPS combines elements of cybernetics, mechatronics, control theory, process science, embedded systems, distributed control, and more recently communication.

Is the Field of Cyber-Physical Systems New?

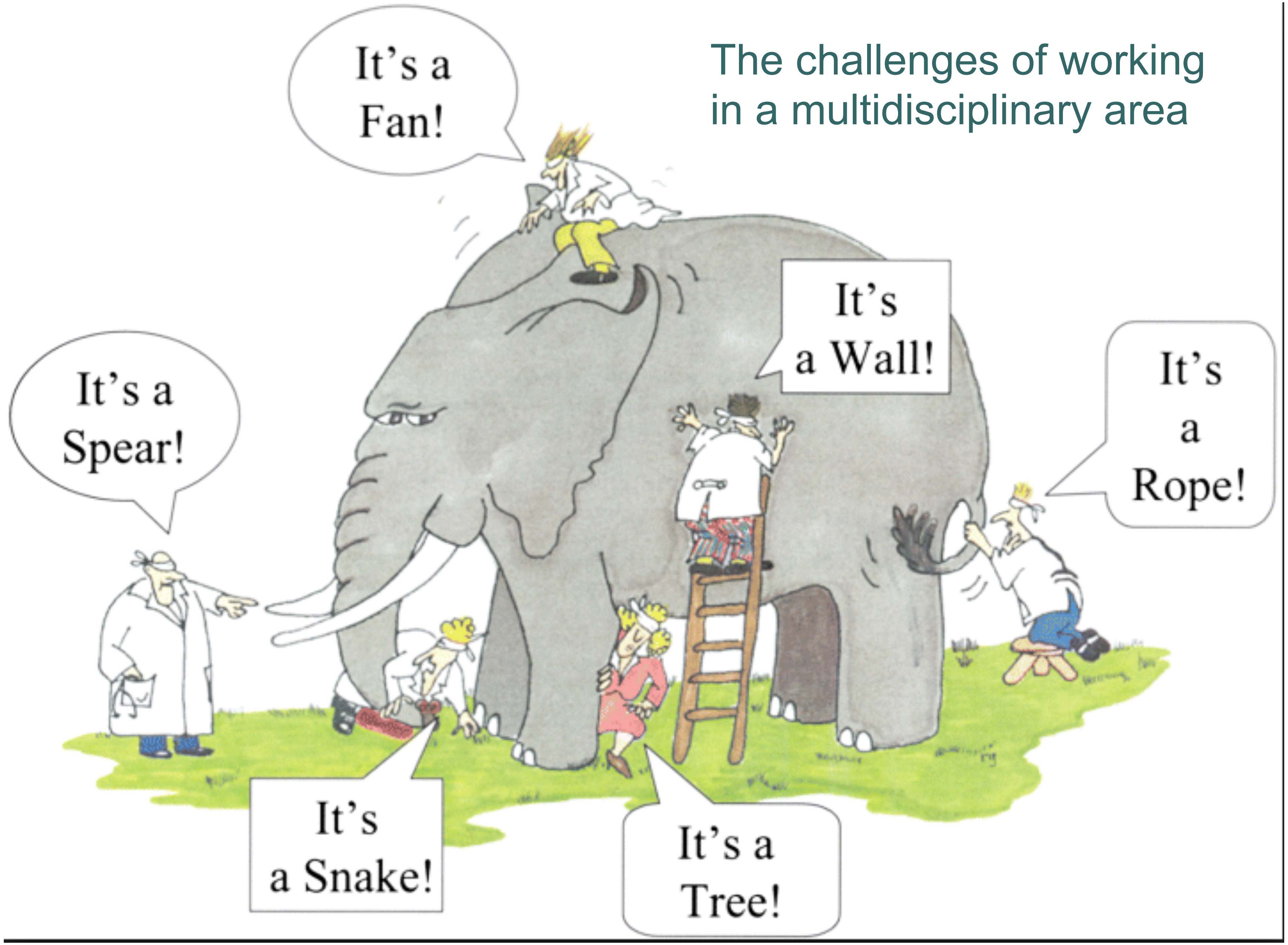
- **Hybrid Systems**: are a mathematical abstraction, CPS are real-world objects.

- **Embedded Systems**: are computational system embedded in a physical system. Any CPS contains an embedded system.

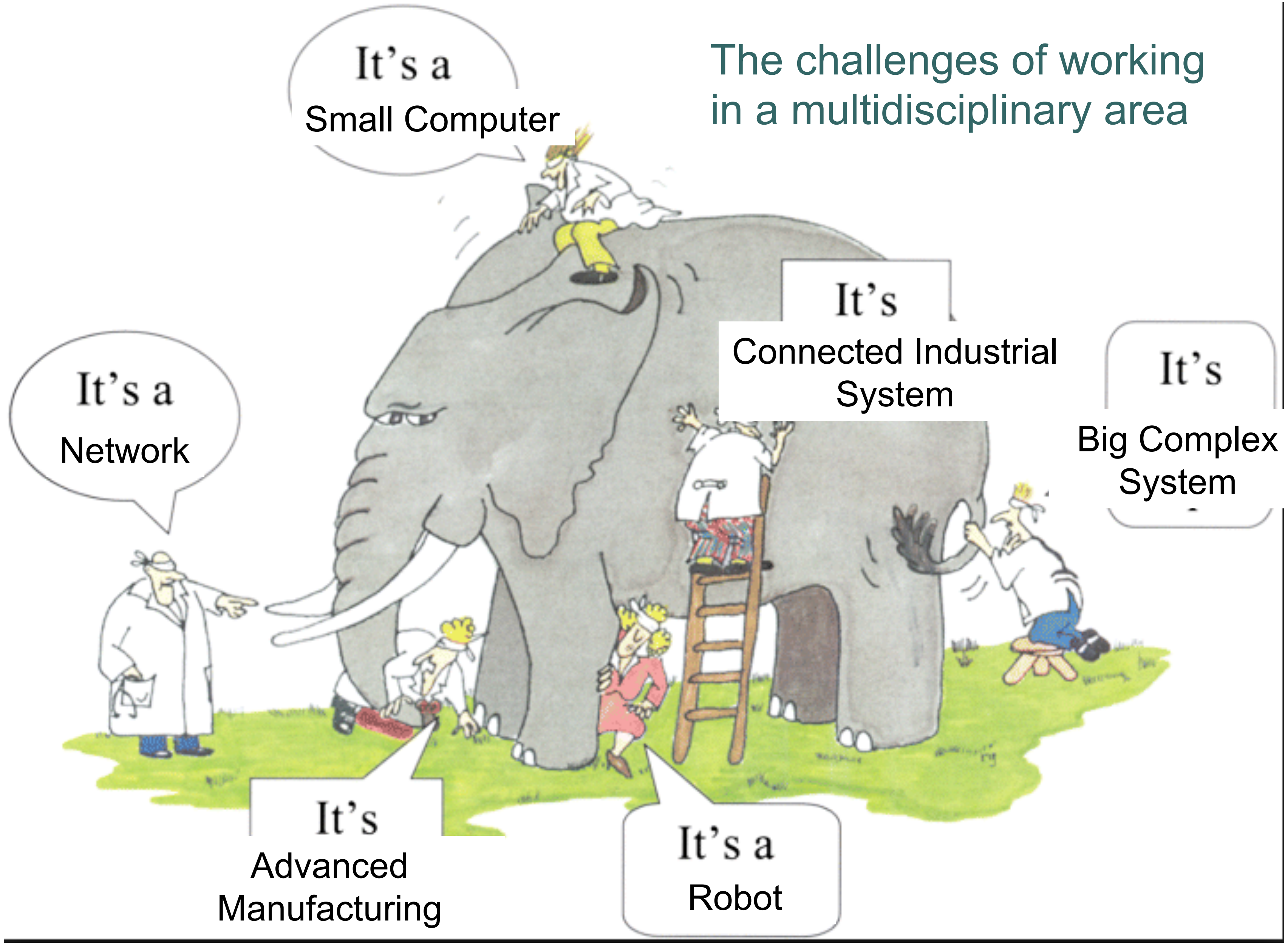
- **Real-time Systems**: must respond to external changes within certain timing constraints. Control systems can have or not real-time constraints.

- Other related disciplines: reliability, multi-agent system, mechanotronics, control theory, robotics, Internet of Things (IoT).

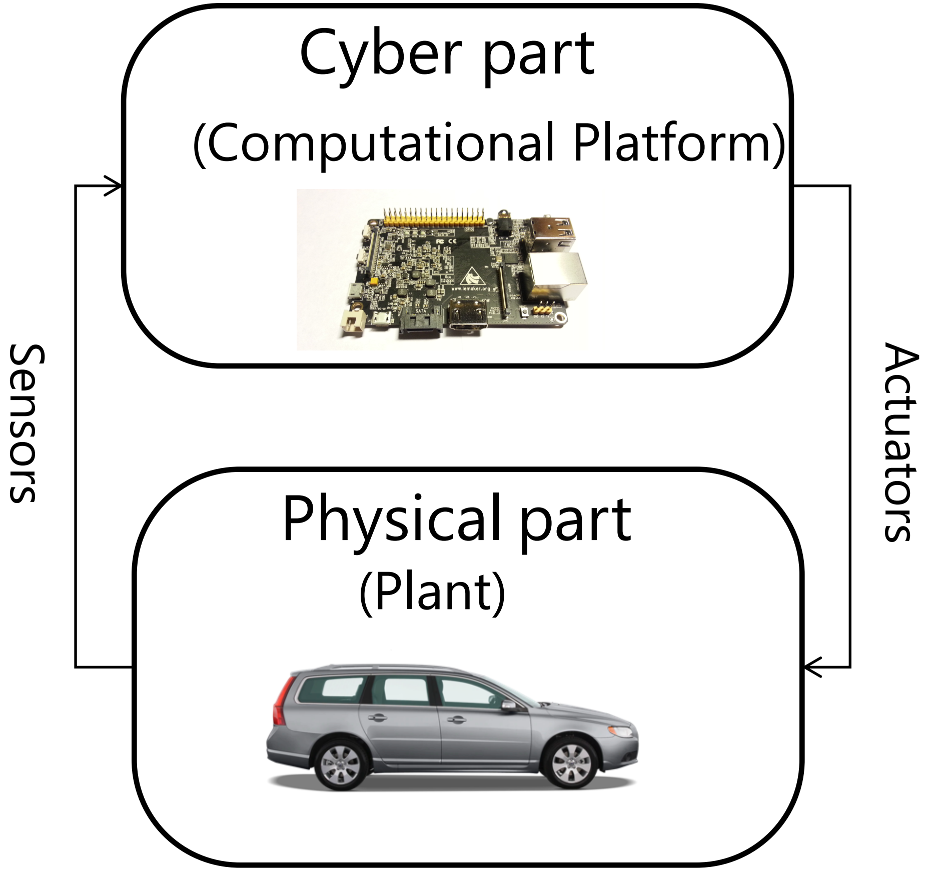
The challenges of working in a multidisciplinary area



The challenges of working in a multidisciplinary area



Example Structure of a CPS



Cyber part

(Computational Platform)

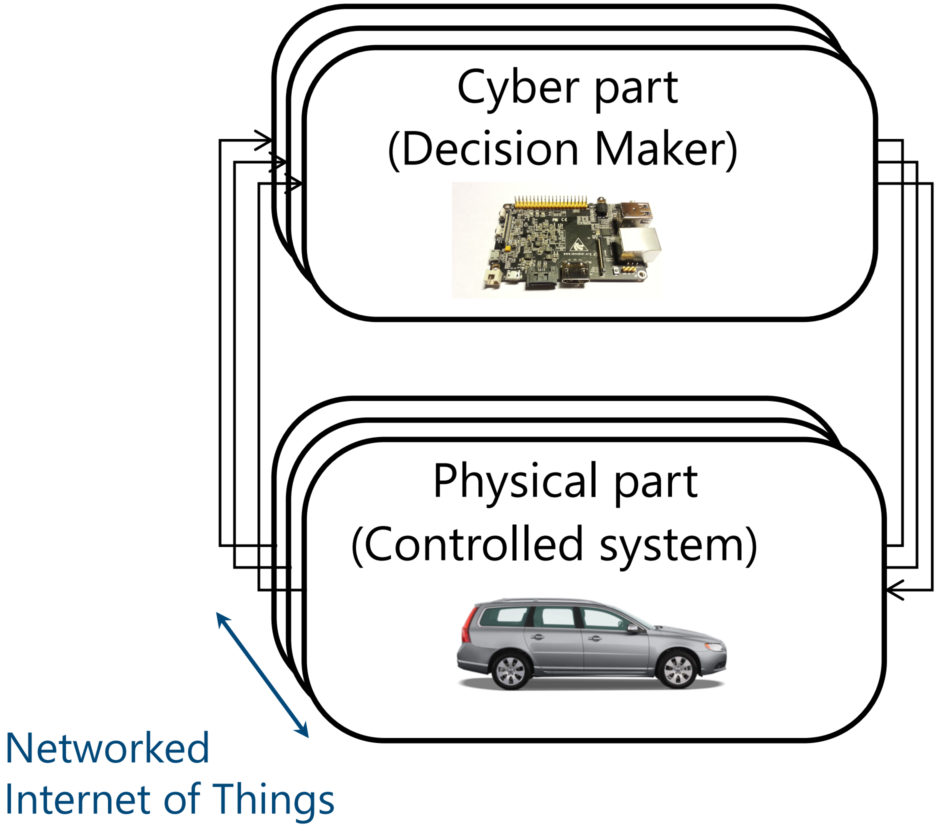
Sensors

Actuators

Physical part

(Plant)

Example Structure of a CPS



Cyber part

(Decision Maker)

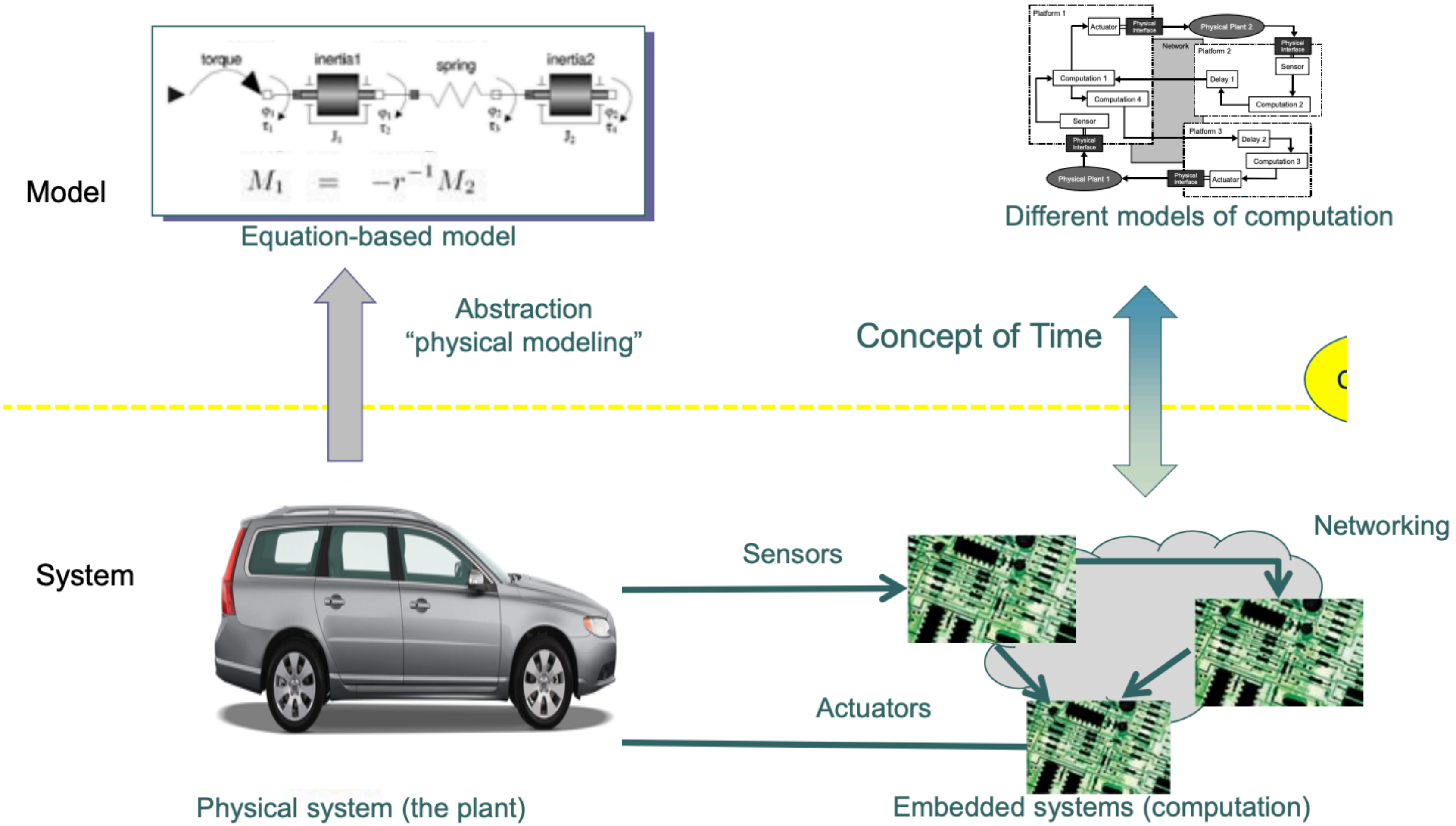
Physical part

(Controlled system)

Networked

Internet of Things

Model-based Design Approach



Model

Equation-based model

Different models of computation

Abstraction
“physical modeling”

Concept of Time

System

Sensors

Networking

Actuators

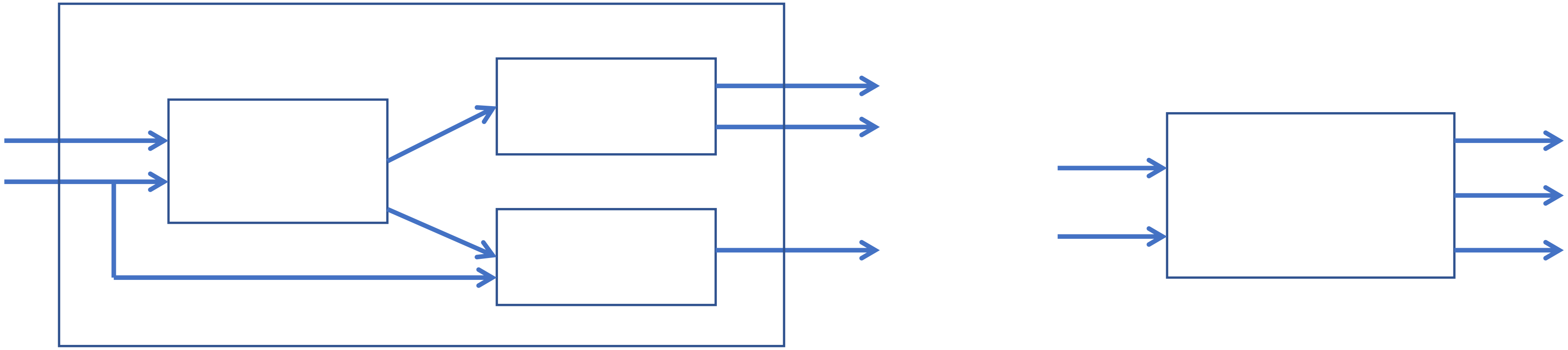
Physical system (the plant)

Embedded systems (computation)

Courtesy: D. Broman

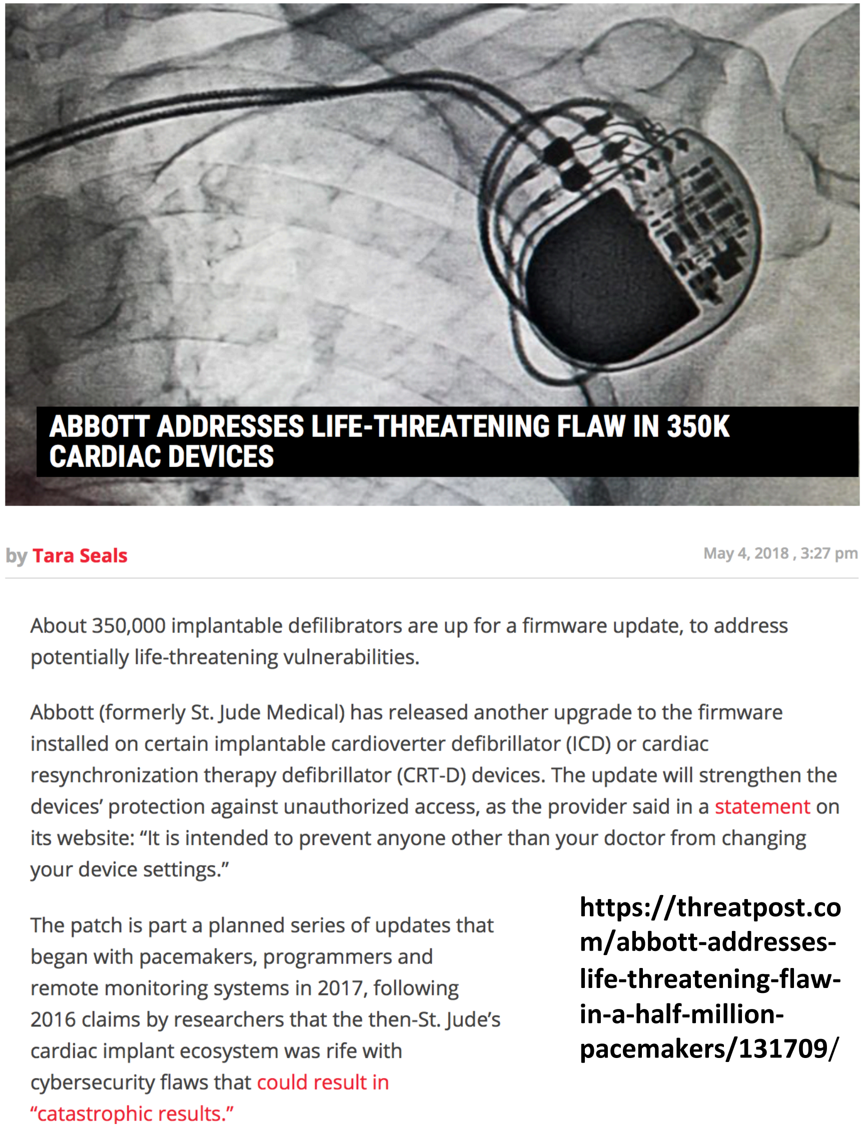
Model-based Design Approach

- MBD when used for designing embedded software[1] has 4 main steps
  1. Model the physical components/environment (also known as a plant model)
  2. Analyze the plant, and synthesize/design the control-software at a high-level
  3. Co-Simulate the plant and control-software
  4. Automatically generate code from the control-software model for deployment
- MBD languages are often visual and block-diagram based, e.g. Simulink



[1] Nicolescu, Gabriela; Mosterman, Pieter J., eds. (2010). Model-Based Design for Embedded Systems. Computational Analysis, Synthesis, and Design of Dynamic Systems. 1. Boca Raton: CRC Press.

Are we safe ?



ABBOTT ADDRESSES LIFE-THREATENING FLAW IN 350K CARDIAC DEVICES

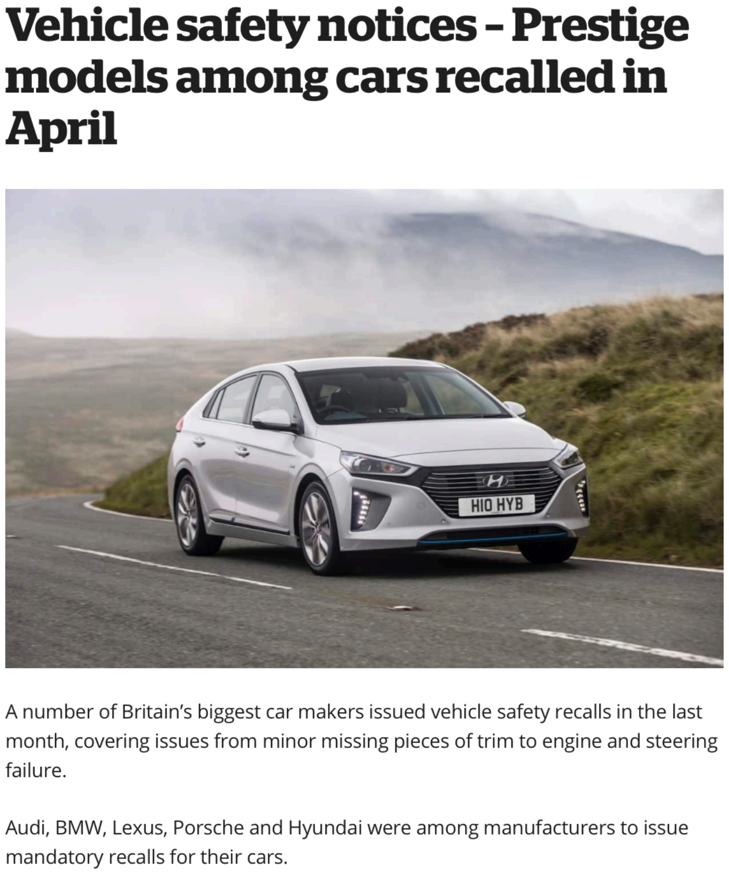
by Tara Seals May 4, 2018 , 3:27 pm

About 350,000 implantable defilibrators are up for a firmware update, to address potentially life-threatening vulnerabilities.

Abbott (formerly St. Jude Medical) has released another upgrade to the firmware installed on certain implantable cardioverter defibrillator (ICD) or cardiac resynchronization therapy defibrillator (CRT-D) devices. The update will strengthen the devices' protection against unauthorized access, as the provider said in a statement on its website: "It is intended to prevent anyone other than your doctor from changing your device settings."

The patch is part a planned series of updates that began with pacemakers, programmers and remote monitoring systems in 2017, following 2016 claims by researchers that the then-St. Jude's cardiac implant ecosystem was rife with cybersecurity flaws that could result in "catastrophic results."

https://threatpost.com/abbott-addresses-life-threatening-flaw-in-a-half-million-pacemakers/131709/



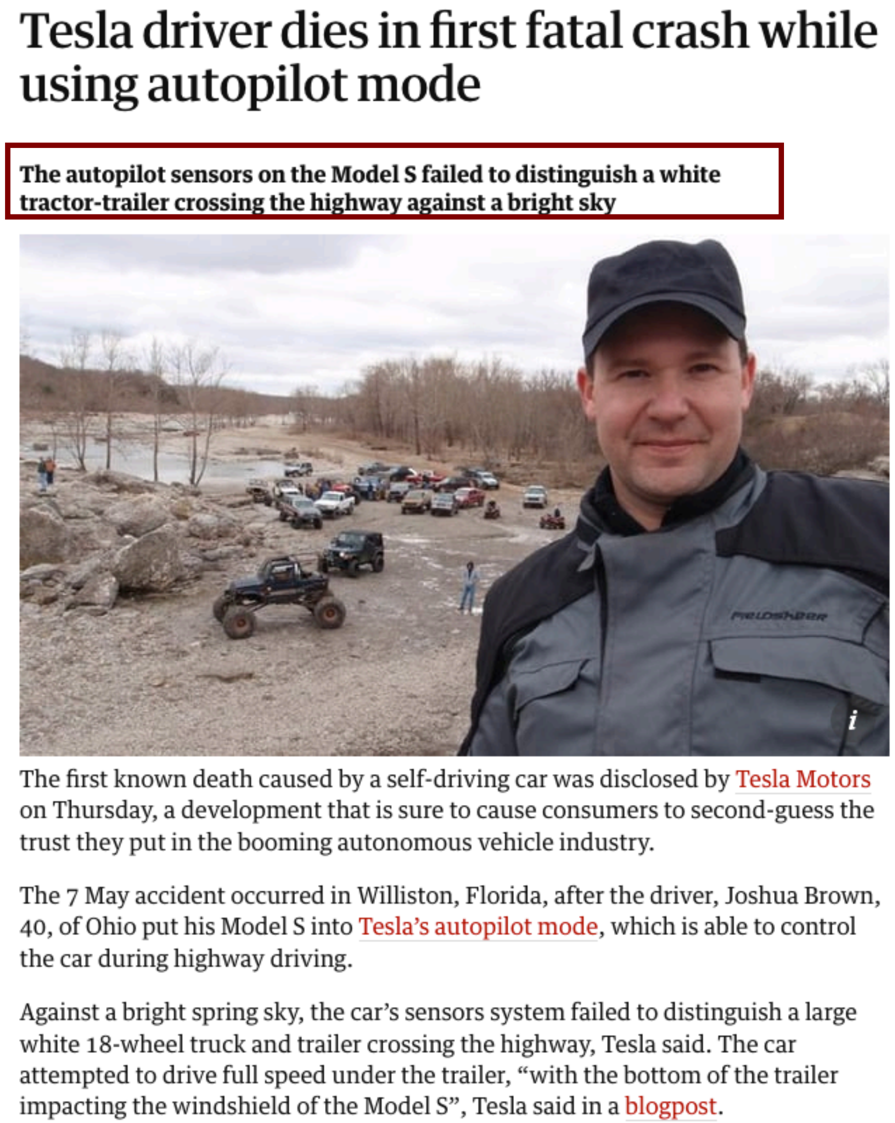
Vehicle safety notices – Prestige models among cars recalled in April

A number of Britain's biggest car makers issued vehicle safety recalls in the last month, covering issues from minor missing pieces of trim to engine and steering failure.

Audi, BMW, Lexus, Porsche and Hyundai were among manufacturers to issue mandatory recalls for their cars.

https://inews.co.uk/essentials/lifestyle/cars/car-news/vehicle-safety-recalls-notices-prestige-cars-recalled-april/

Some tragic accidents



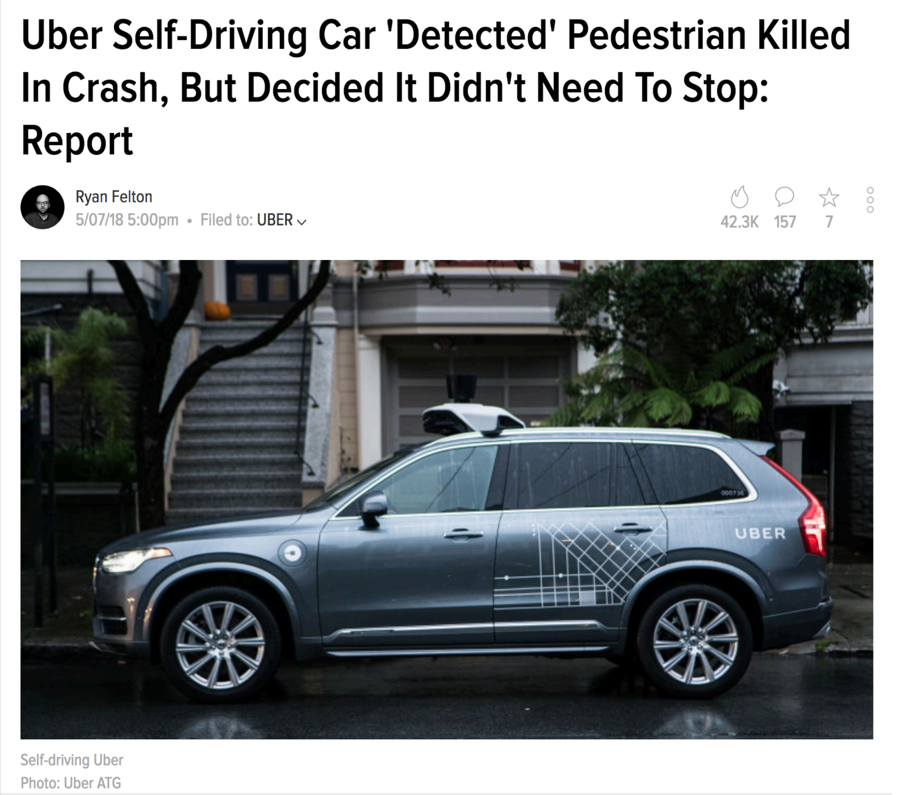
Tesla driver dies in first fatal crash while using autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky

The first known death caused by a self-driving car was disclosed by Tesla Motors on Thursday, a development that is sure to cause consumers to second-guess the trust they put in the booming autonomous vehicle industry.

The 7 May accident occurred in Williston, Florida, after the driver, Joshua Brown, 40, of Ohio put his Model S into Tesla's autopilot mode, which is able to control the car during highway driving.

Against a bright spring sky, the car's sensors system failed to distinguish a large white 18-wheel truck and trailer crossing the highway, Tesla said. The car attempted to drive full speed under the trailer, "with the bottom of the trailer impacting the windshield of the Model S", Tesla said in a blogpost.

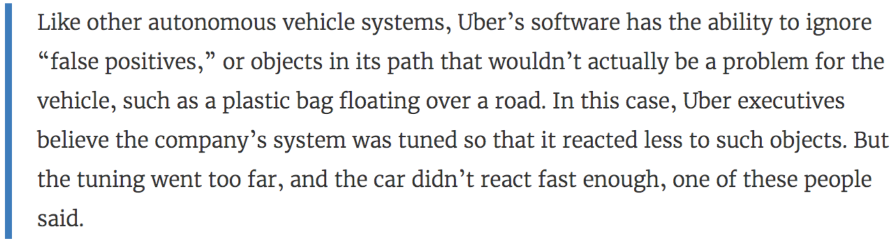


Uber Self-Driving Car 'Detected' Pedestrian Killed In Crash, But Decided It Didn't Need To Stop: Report

Ryan Felton
5/07/18 5:00pm • Filed to: UBER

42.3K 157 7

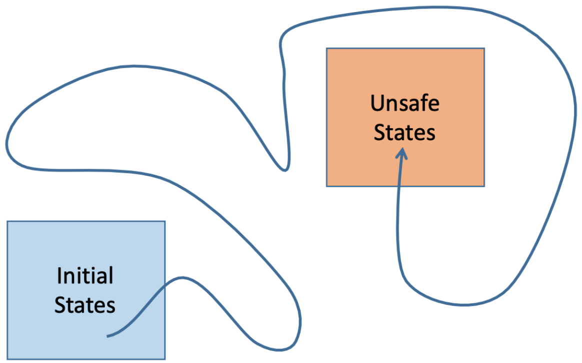
Self-driving Uber
Photo: Uber ATG



> Like other autonomous vehicle systems, Uber's software has the ability to ignore "false positives," or objects in its path that wouldn't actually be a problem for the vehicle, such as a plastic bag floating over a road. In this case, Uber executives believe the company's system was tuned so that it reacted less to such objects. But the tuning went too far, and the car didn't react fast enough, one of these people said.

https://jalopnik.com/uber-self-driving-car-detected-pedestrian-killed-in-cra-1825834016

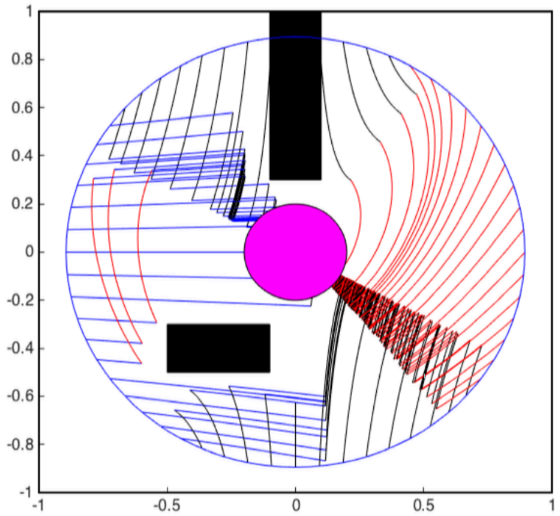
Reachability



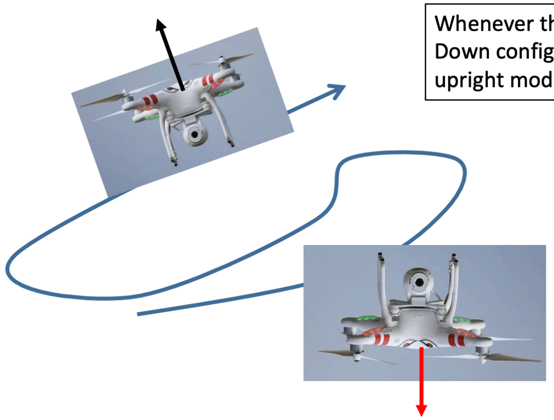
Unsafe States

Initial States

Stability



Real-Time Temporal Properties



Whenever the UAV reaches an Upside-Down configuration, it must reach an upright mode within 2 seconds.

Formal Reasoning

Formal Methods

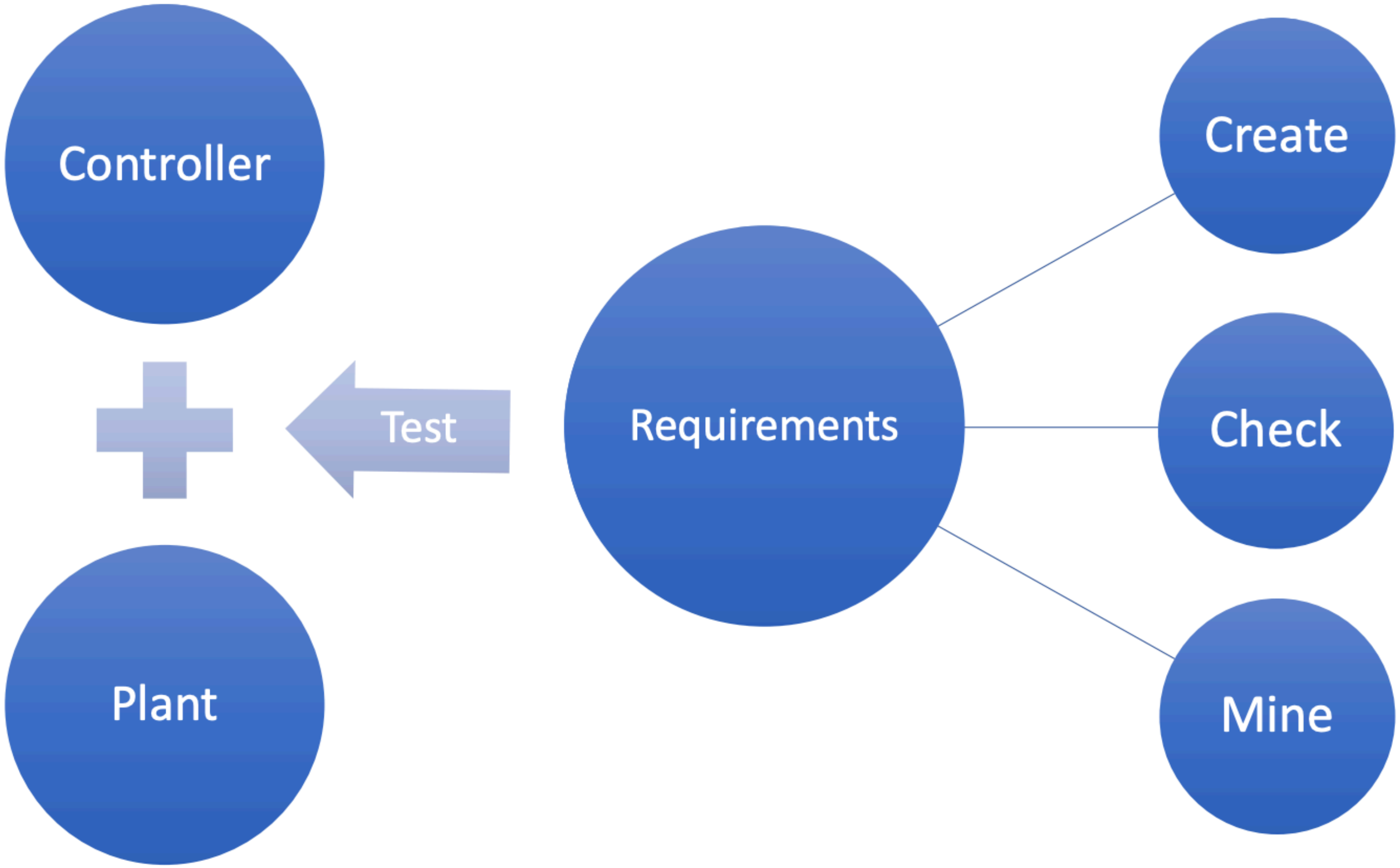
Mathematical, Algorithmic techniques for modeling, design, analysis

– **Specification**: WHAT the system must/must not do

– **Verification**: WHY it meets the spec (or not)

– **Synthesis**: HOW it meets the spec (correct-by-construction design)

Requirement-Driven Design



Requirements formally capture what it means for a system to operate correctly in its operating environment

Requirement-Driven Design

Exhaustive verification of CPS is increasingly intractable:

- Openness, environmental change
- Uncertainty, spatial distribution
- Emergent behaviors resulting from the local interactions are not predictable by the analysis of system's individual parts
- Classic state-space explosion problem

How to ensure safety-critical requirements in CPS ?

Course Objectives

- Gain basic familiarity with CPS topics

  Challenge Problems/Case studies

- “Model-Based” Software Development Paradigm for CPS

  Developing models for physical components (+ software + communication)

- Writing checkable requirements and tests

- Reinforcement Learning for CPS Safety Engineering?

Course Overview

1. Intro to CPS and application domains with example (e.g. Medical CPS, energy CPS, transportation CPS)

2. **Modeling formalism**: ODE systems, Timed Automata, hybrid and switching systems, Stochastic Hybrid Automata, Markov Decision Process (MDP).

3. **Verification\Monitoring:** temporal logic and automata, Model Checking , Run-time Verification, Reachability Analysis, Test Generation, Falsification

4. **Reinforcement Learning** for CPS (and formal methods)

Books

- Principles of Cyber-Physical Systems, Rajeev Alur, MIT Press, 2015
- Introduction to Embedded Systems: A CPS approach
  Free at: https://ptolemy.berkeley.edu/books/leeseshia/
- Principle of Model Cheking, Baier, Katoen, MIT Press, 2008
- Reinforcement Learning, An Introduction, RS Sutton, AG Barton, Cambridge, 2011

Grading

Project with a practice development of a CPS application, verification of formal requirements and falsification or test generation experiments

- Matlab/Simulink (simulation) model of a CPS application
- Can also develop model in Python or Java if that is the preferred language (will require additional work for handling requirements but I can help you!)
- Hypro (Toolbox for the Reachability Analysis of Hybrid Systems)
- Open to other software solution

Oral exam with presentation of the Project