Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste
II Semestre 2018

Lecture 1: Introduction and Course Logistic

Course Logistics

Timing

- Laura: Tue & Thur 11-12:30, aula 4A
- Prof. Jyo Deshmukh: March 27,28
- Prof. Antonio Celani: April 2-18 Tue&Wed&Thur&Friday 9-11:30

Course Website

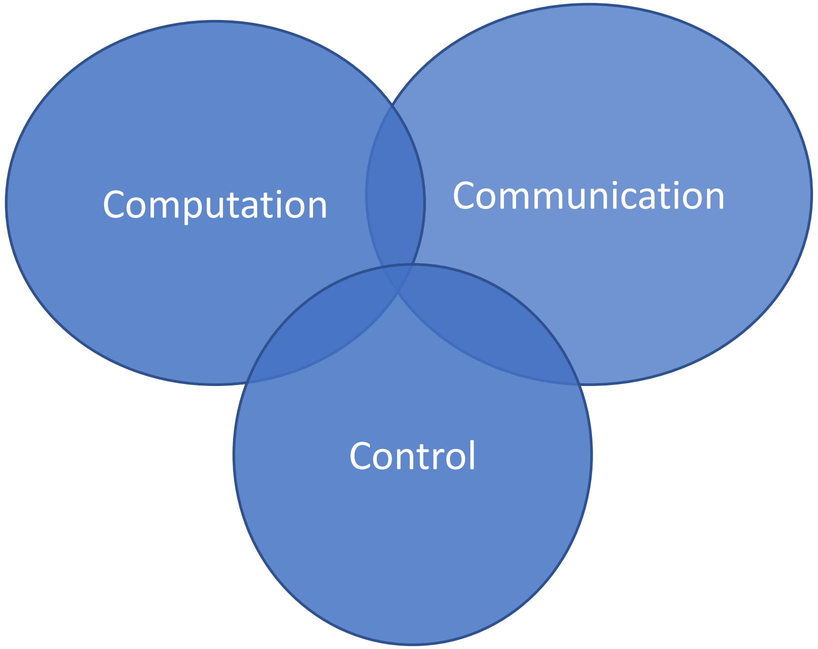
Moodle

What is a Cyber-Physical System?

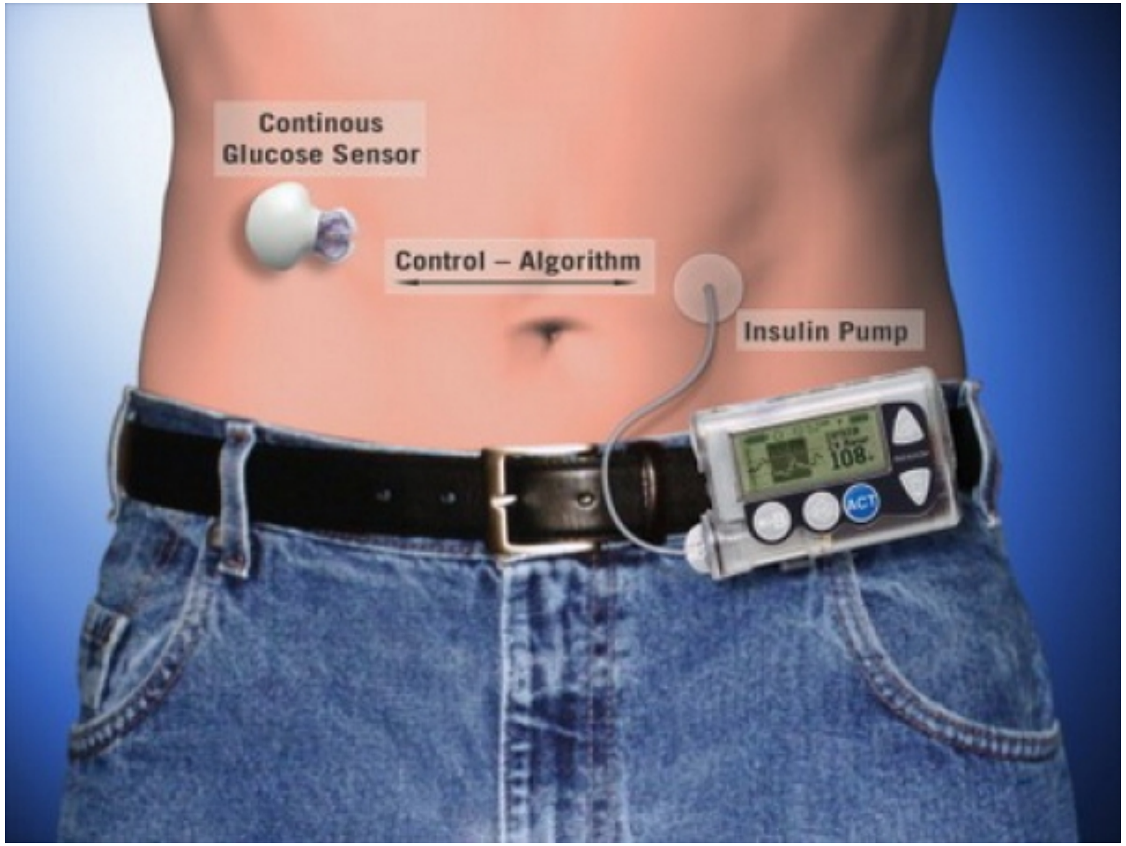
A CPS is a **mechanism** that is controlled or monitored by **computer-based algorithms**, tightly integrated with the Internet and its users.

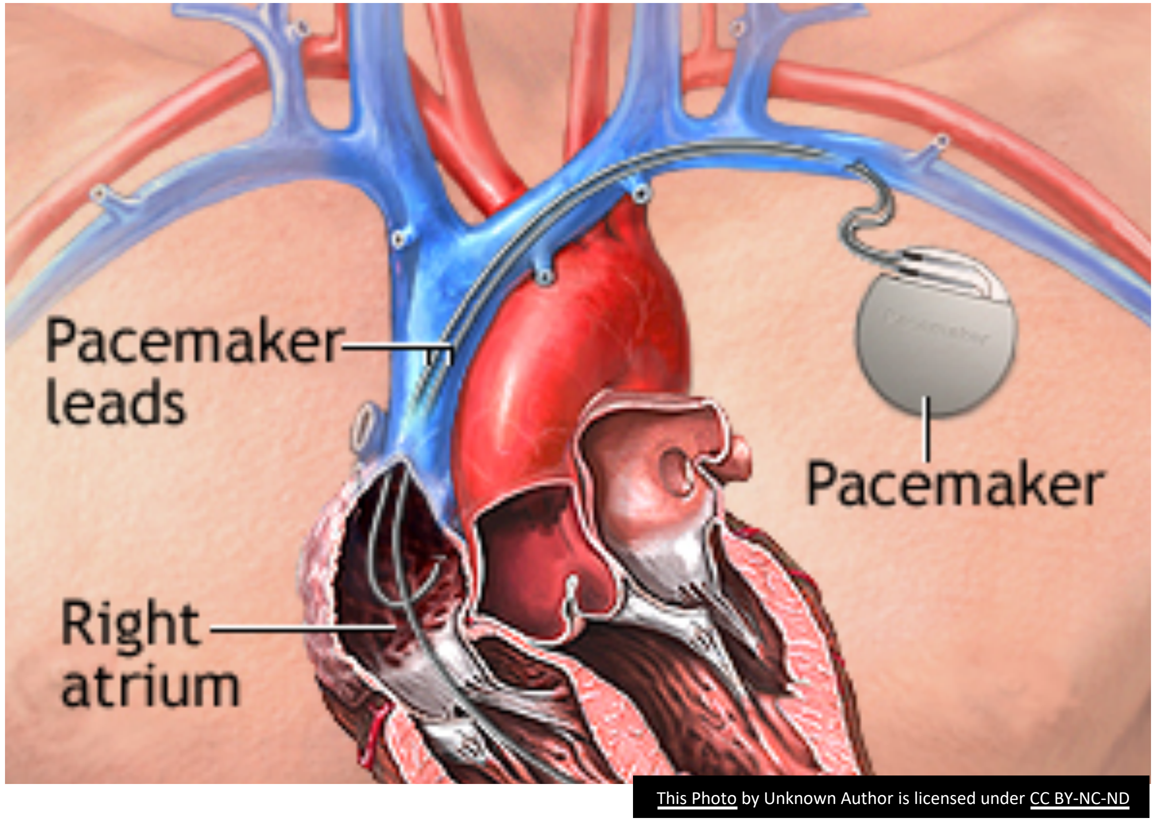
Physical = physical device or system + environment

Cyber = computational + communicational



Medical Device

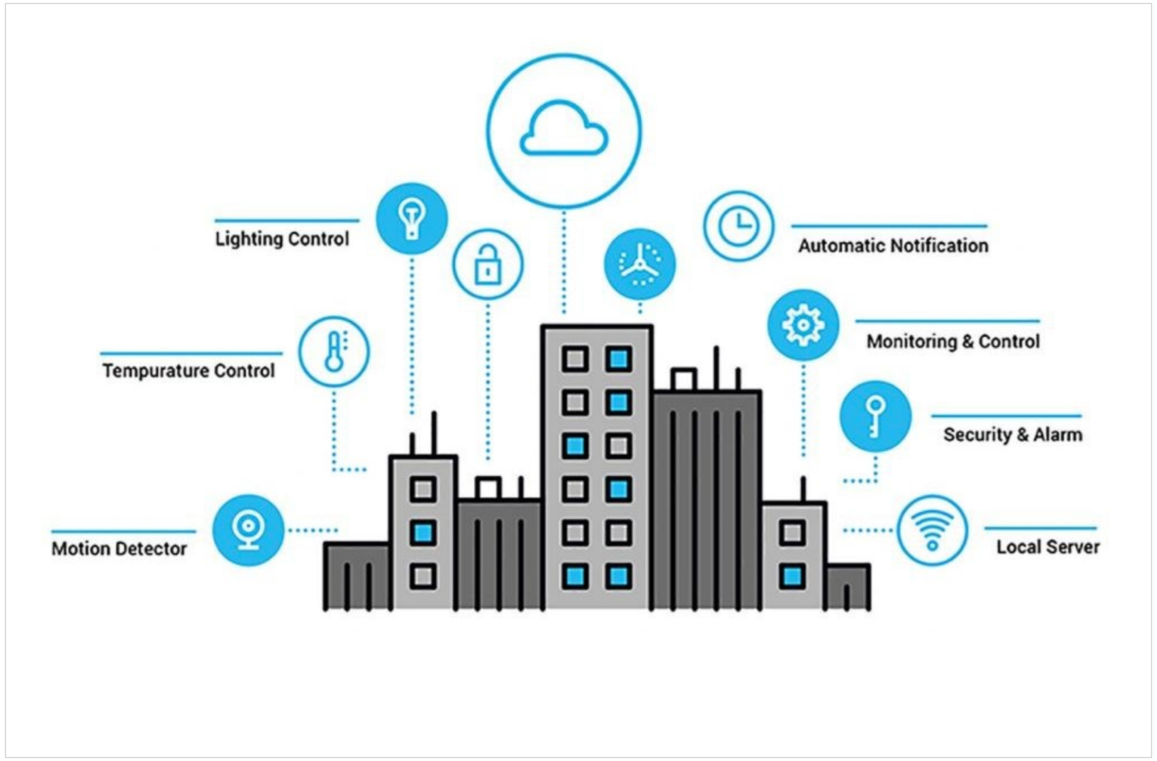




Transportation

Energy

© Siemens


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

And many other applications…

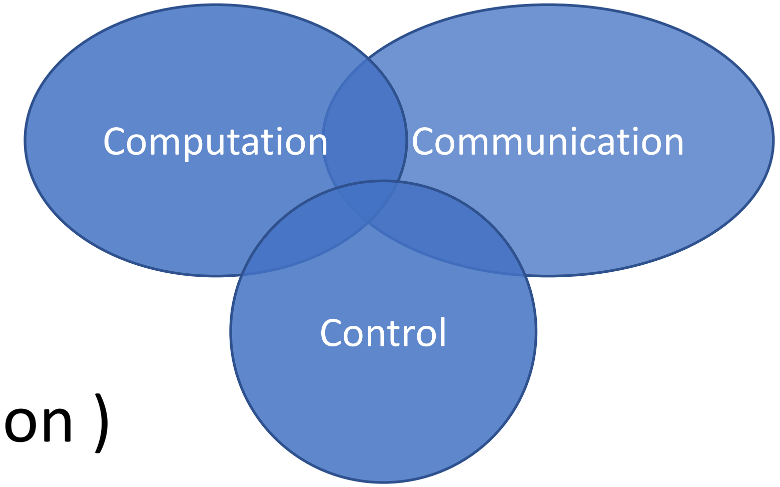
- Robotics
- Critical Infrastructures
- Industrial Control
- Manufactering
- Agricolture

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?

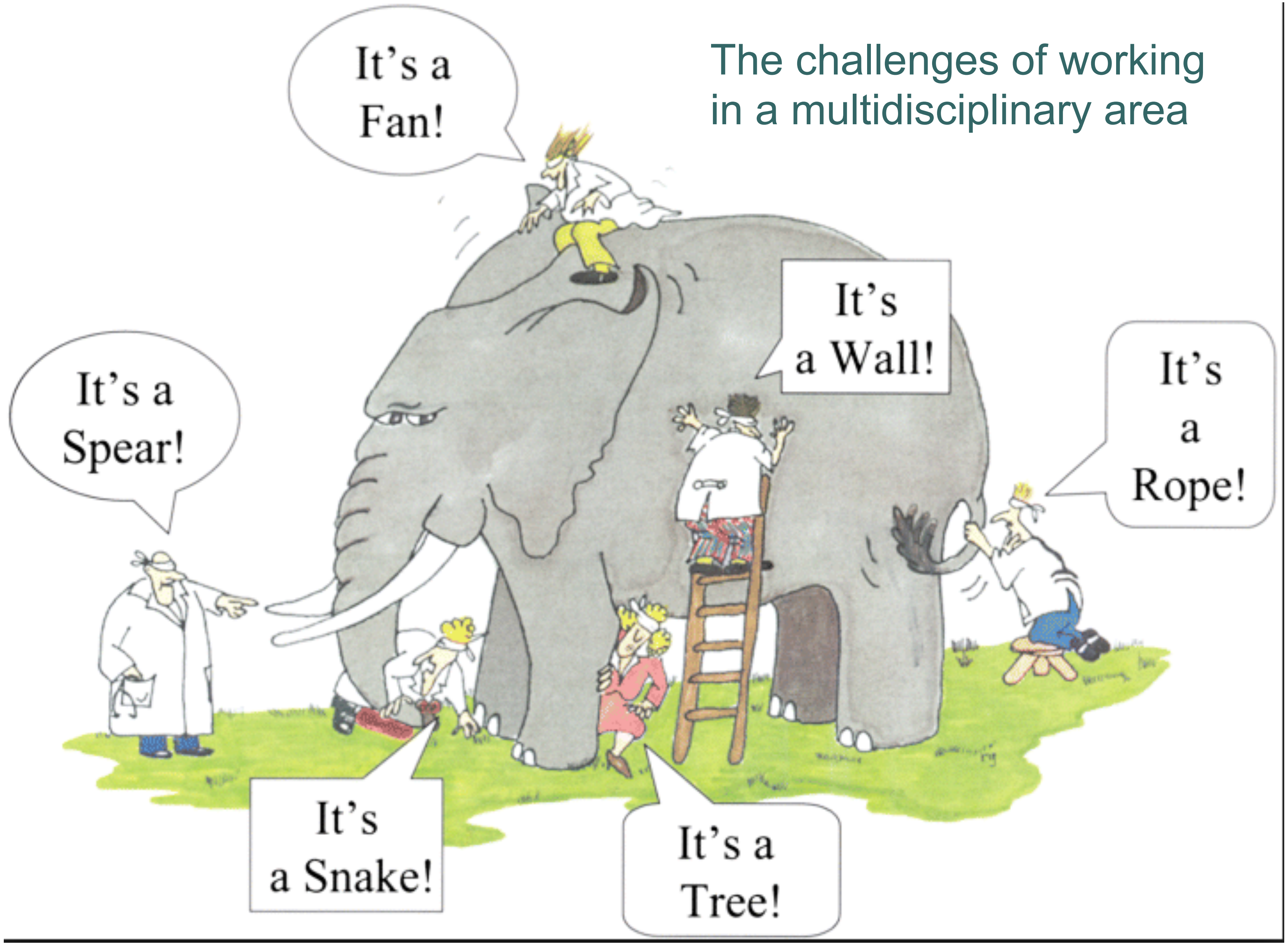
- **Hybrid Systems**: are a mathematical abstraction, CPS are real-world objects.

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

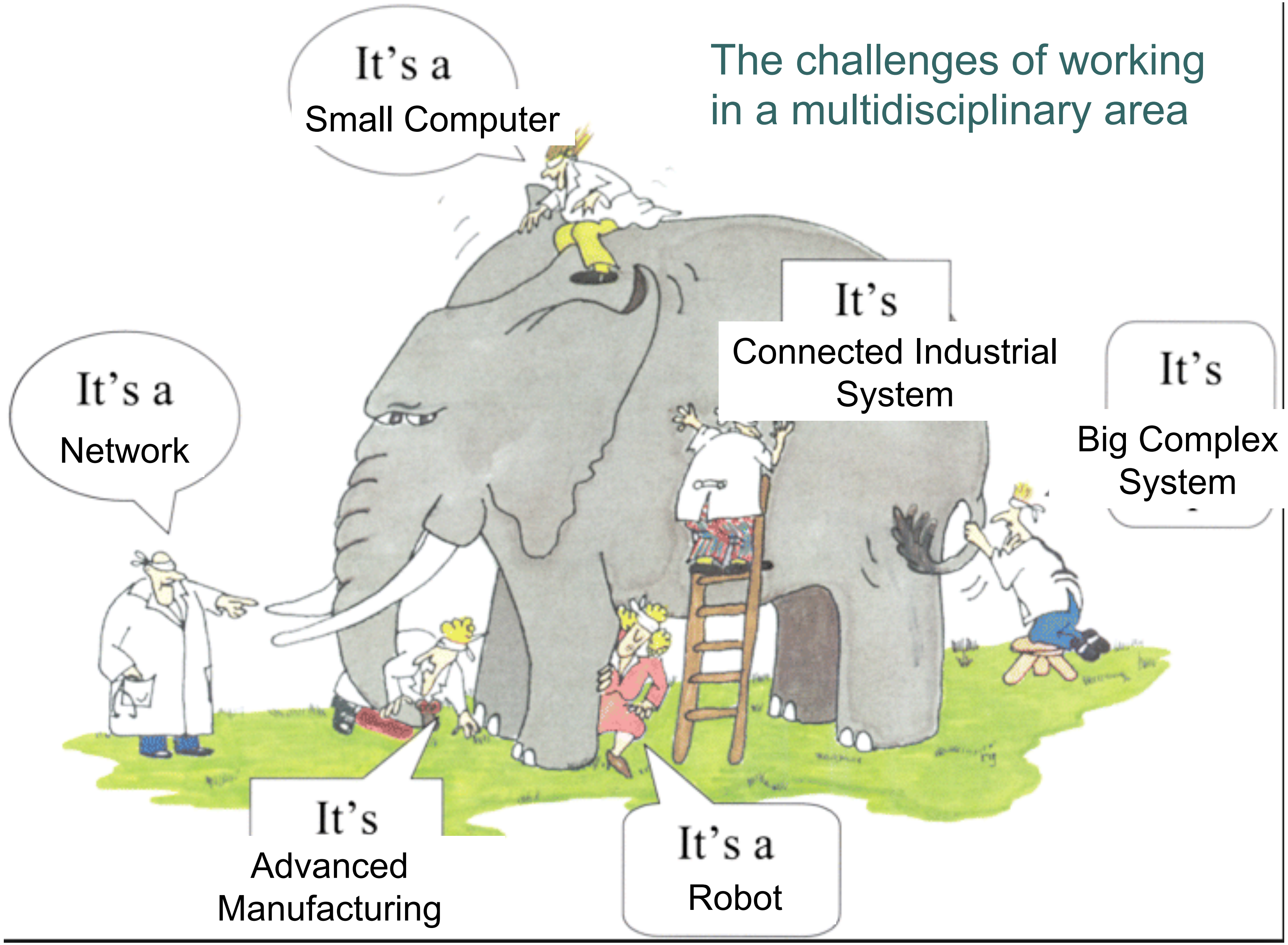
- **Real-time Systems**: must respond to external changes within certain timing constraints. Control systems can have or not real-time constraints.

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

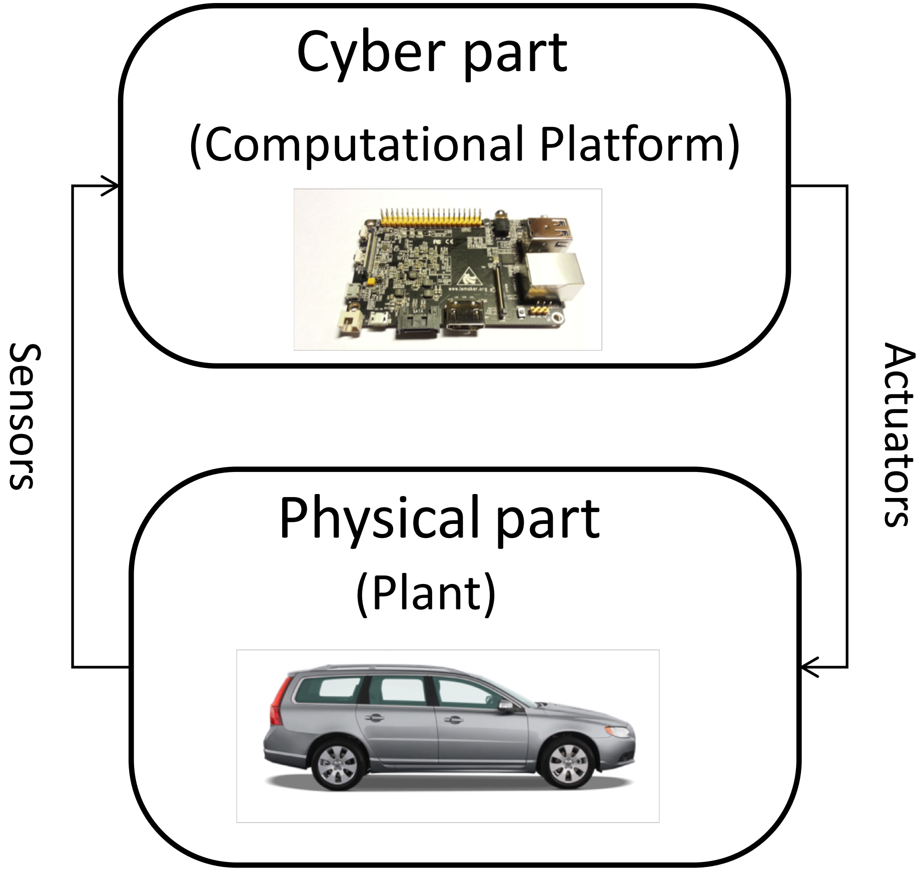
The challenges of working in a multidisciplinary area



The challenges of working in a multidisciplinary area



Example Structure of a CPS



Cyber part

(Computational Platform)

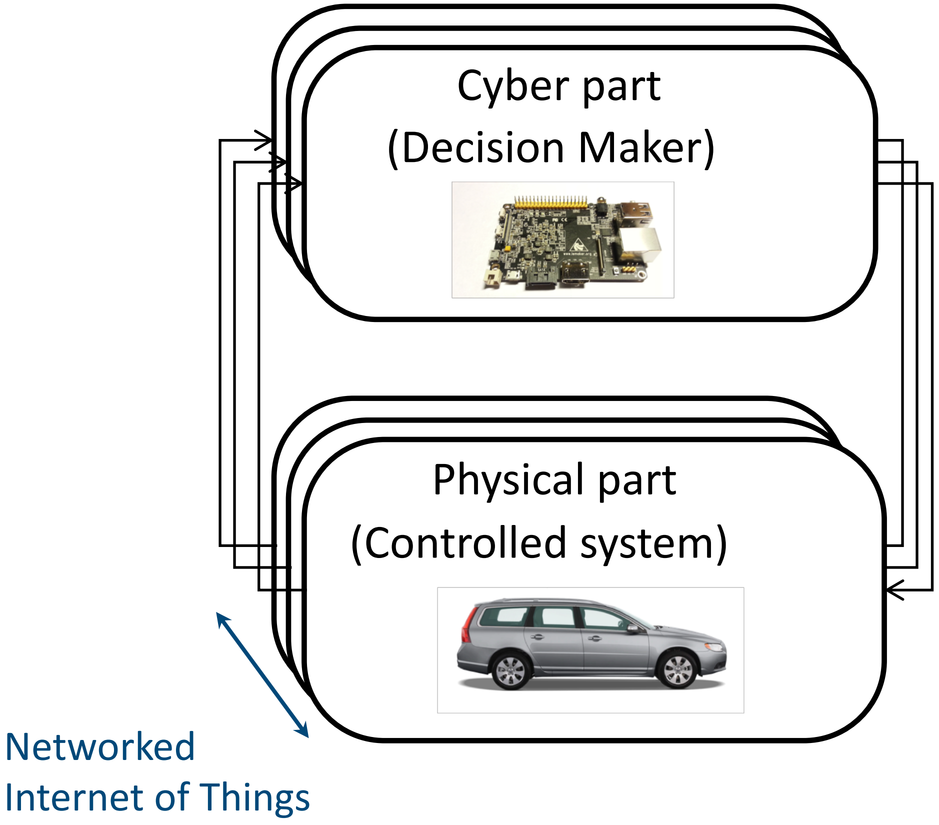
Sensors

Actuators

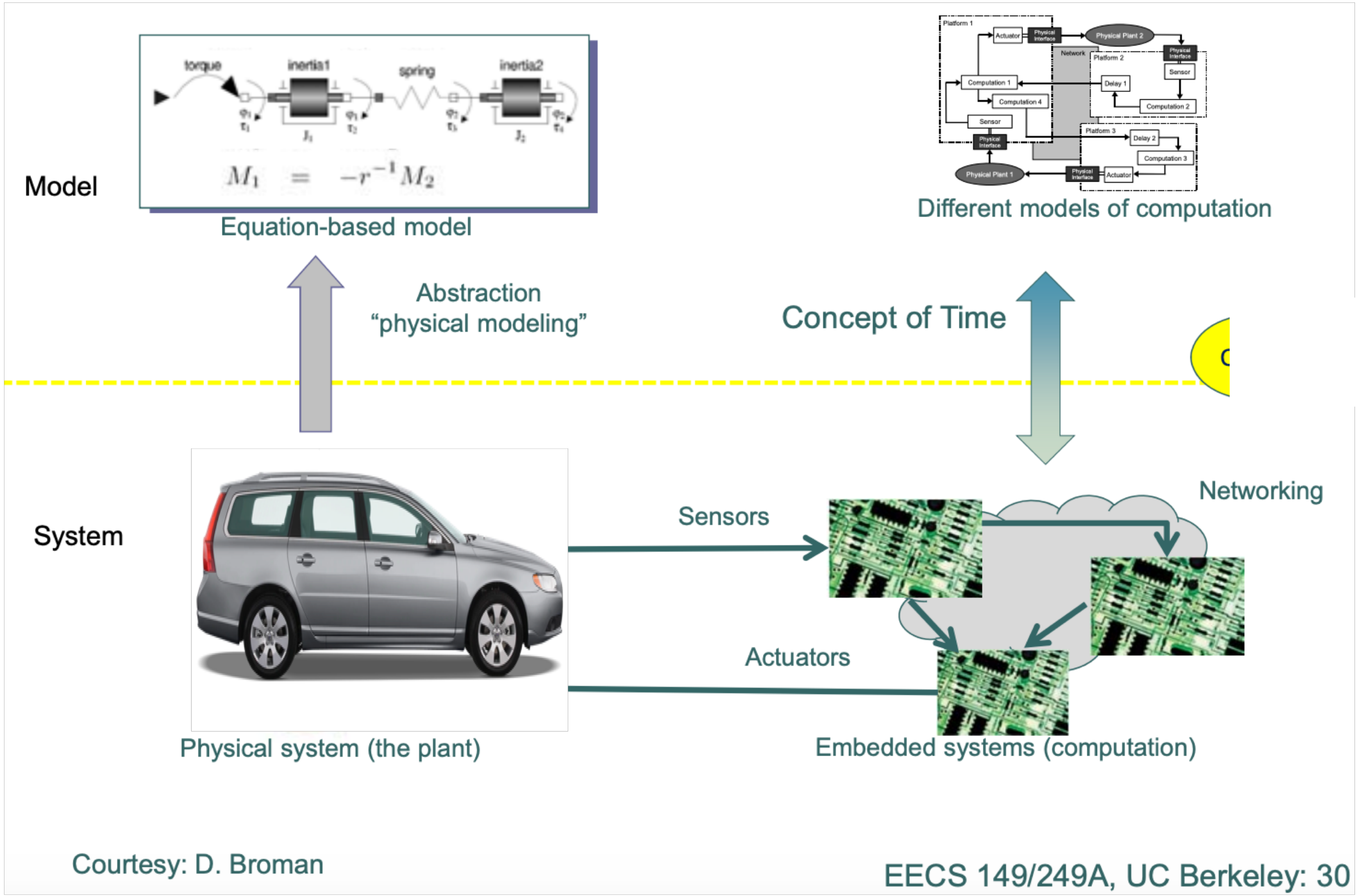
Physical part

(Plant)

Example Structure of a CPS



Model-based Design Approach



Model

$$M_1 = -r^{-1} M_2$$

Equation-based model

Different models of computation

Abstraction
“physical modeling”

Concept of Time

System

Sensors

Networking

Actuators

Physical system (the plant)

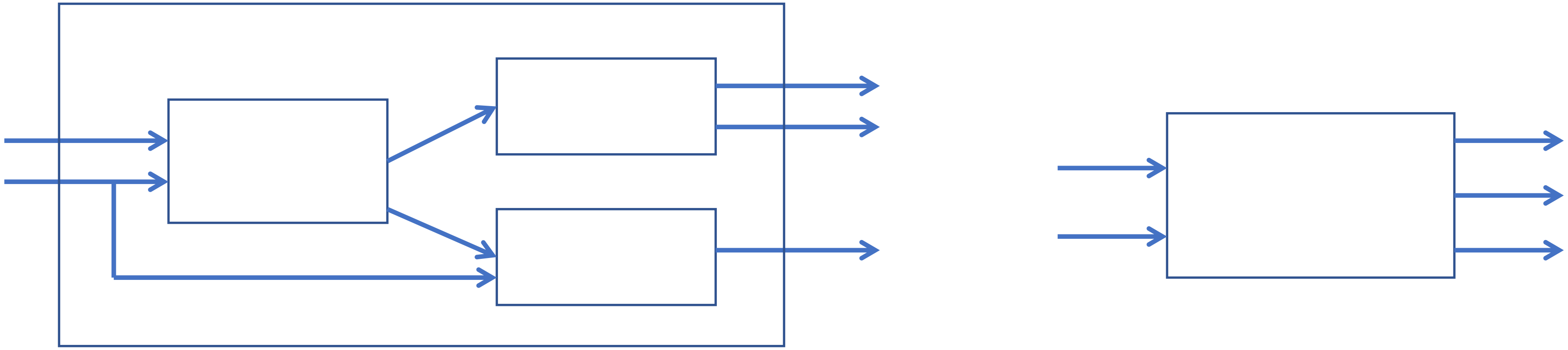
Embedded systems (computation)

Courtesy: D. Broman

EECS 149/249A, UC Berkeley: 30

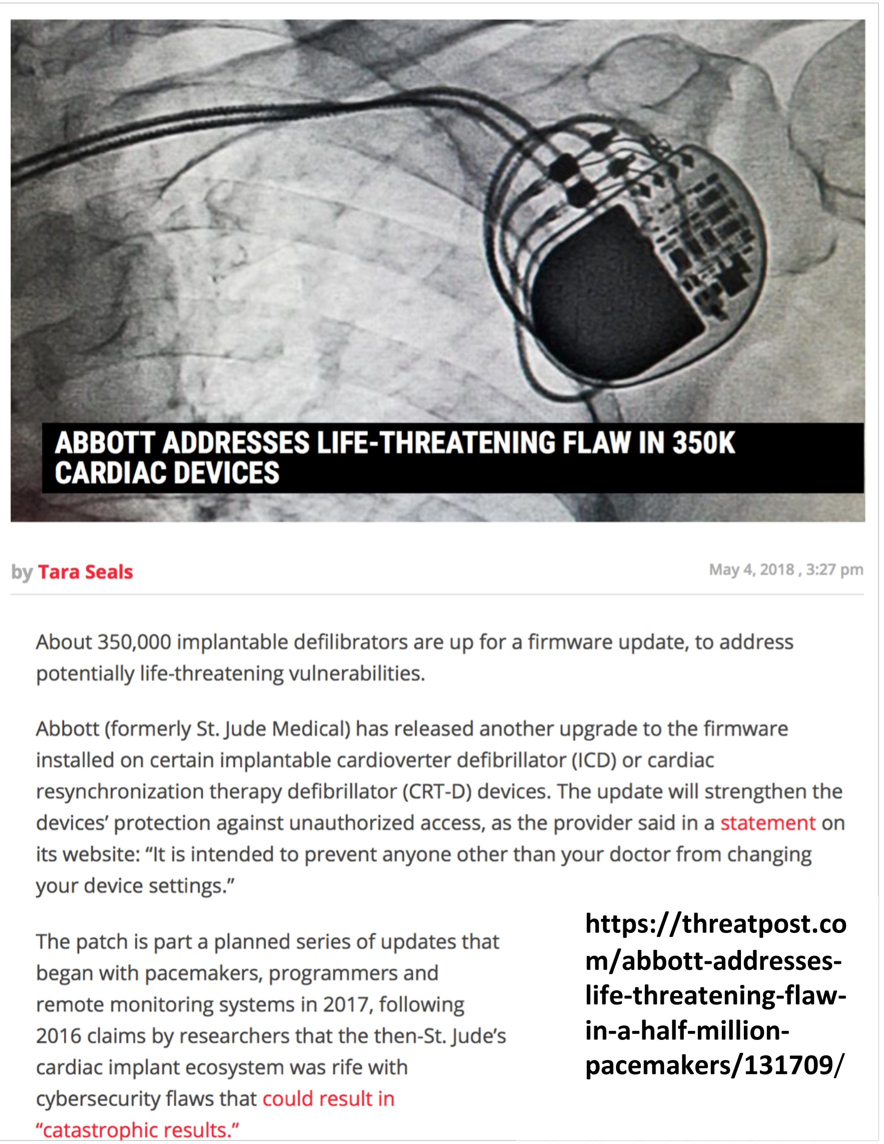
Model-based Design Approach

- 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

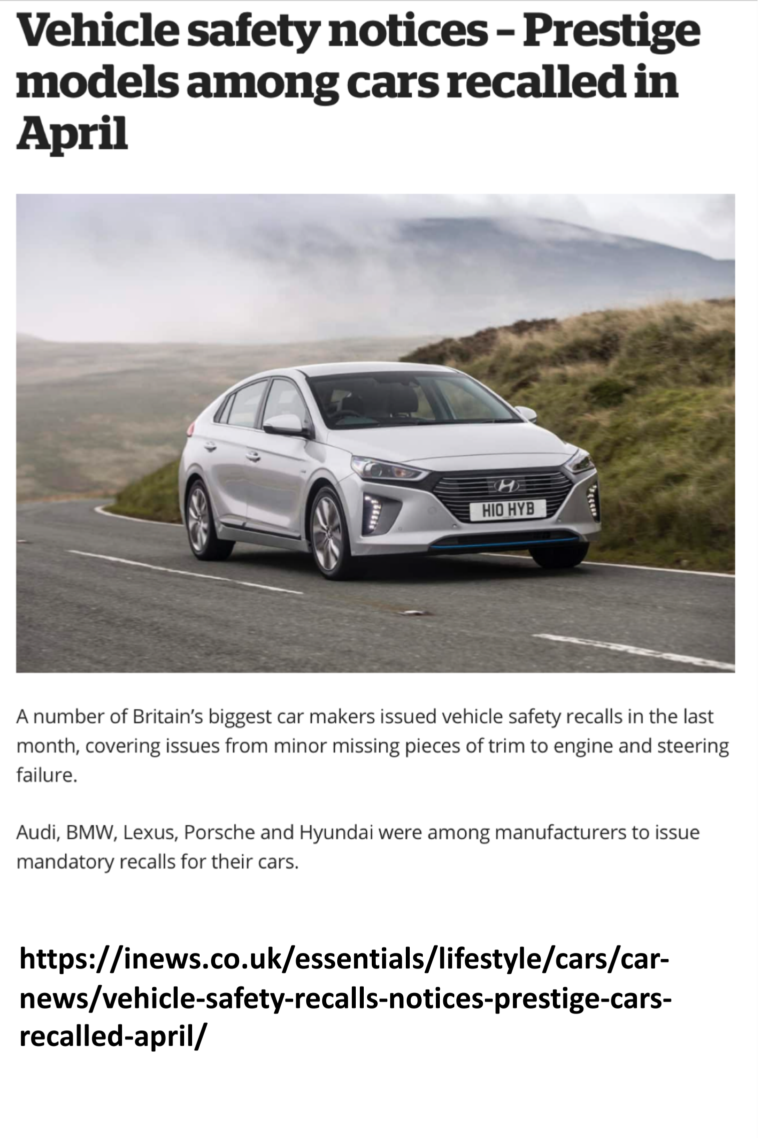
May 4, 2018 , 3:27 pm

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/



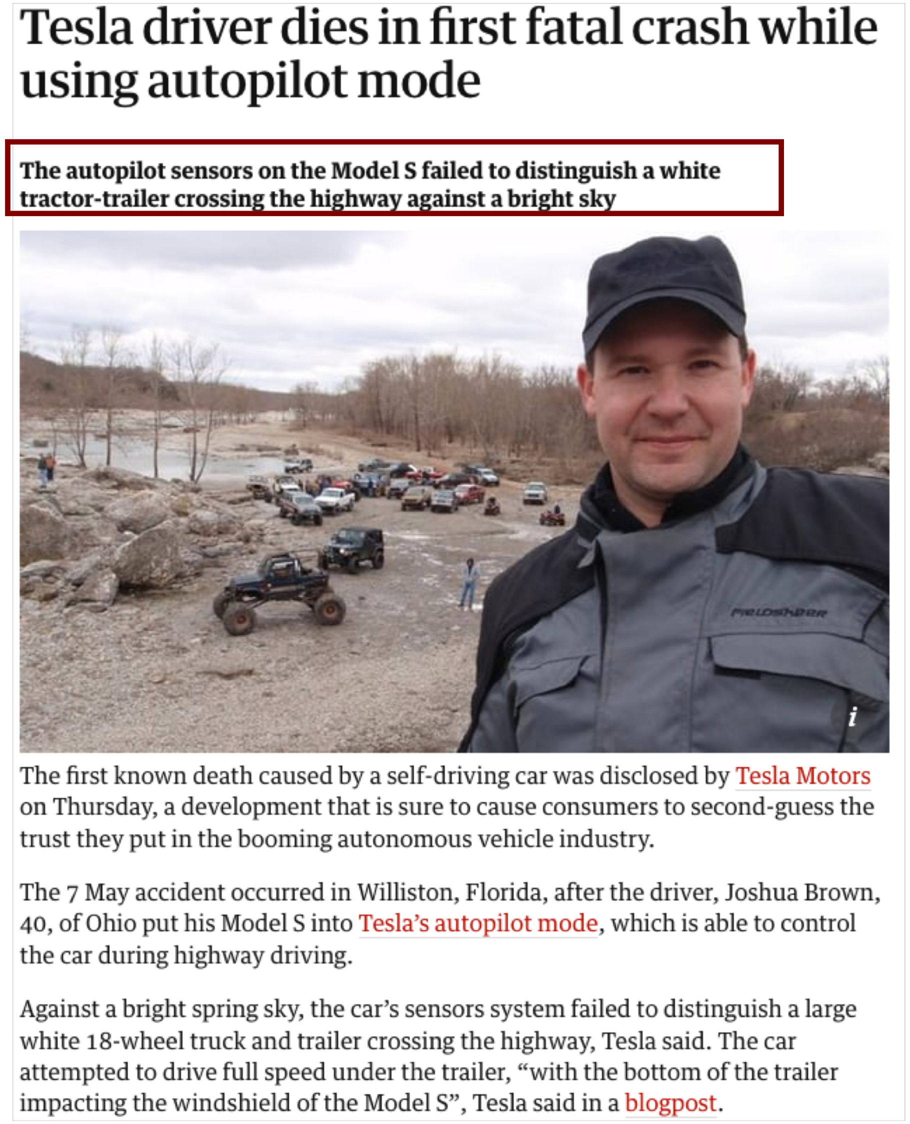
Vehicle safety notices – Prestige models among cars recalled in April

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



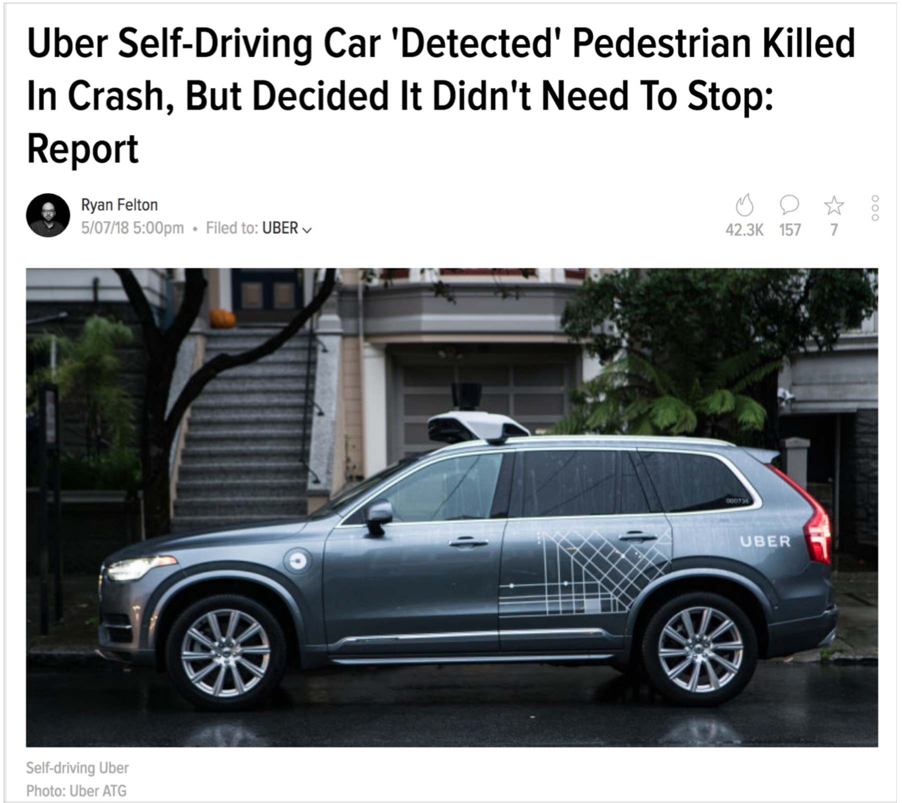
Tesla driver dies in first fatal crash while using autopilot mode

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.

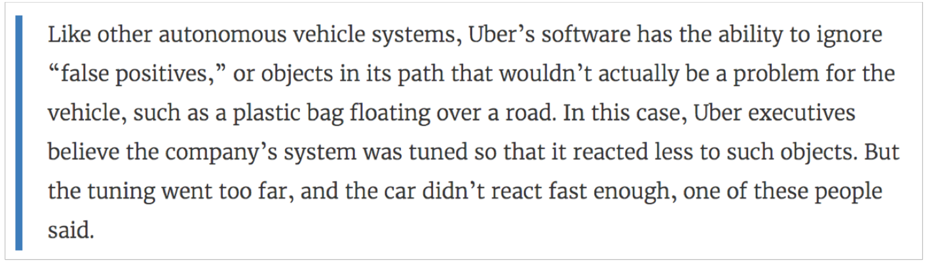
Against a bright spring sky, the car's sensors system failed to distinguish a large white 18-wheel truck and trailer crossing the highway, Tesla said. The car attempted to drive full speed under the trailer, "with the bottom of the trailer impacting the windshield of the Model S", Tesla said in a blogpost.



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

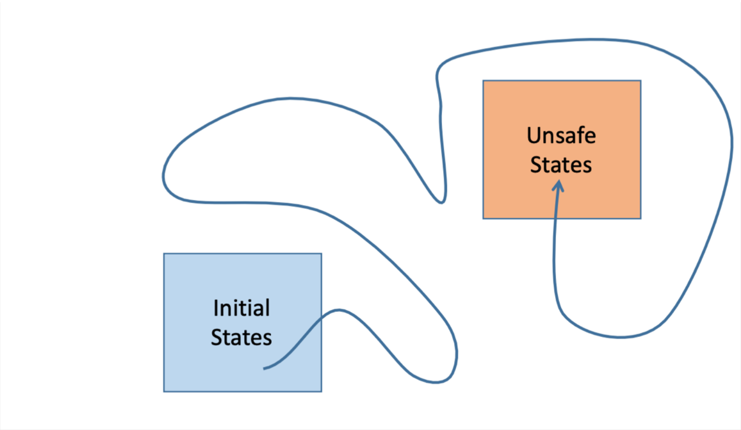
Self-driving Uber
Photo: Uber ATG



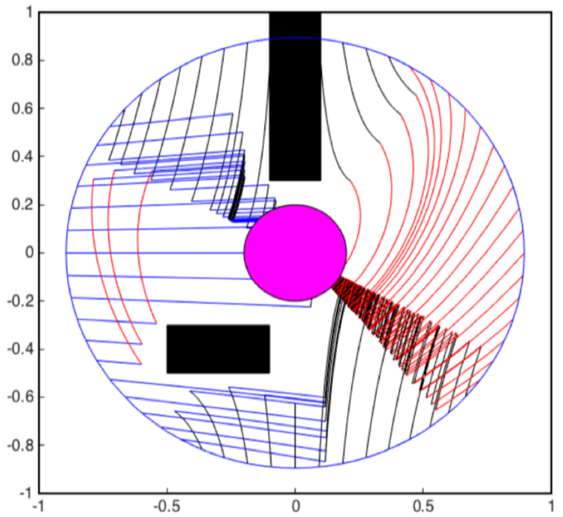
> Like other autonomous vehicle systems, Uber's software has the ability to ignore "false positives," or objects in its path that wouldn't actually be a problem for the vehicle, such as a plastic bag floating over a road. In this case, Uber executives believe the company's system was tuned so that it 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

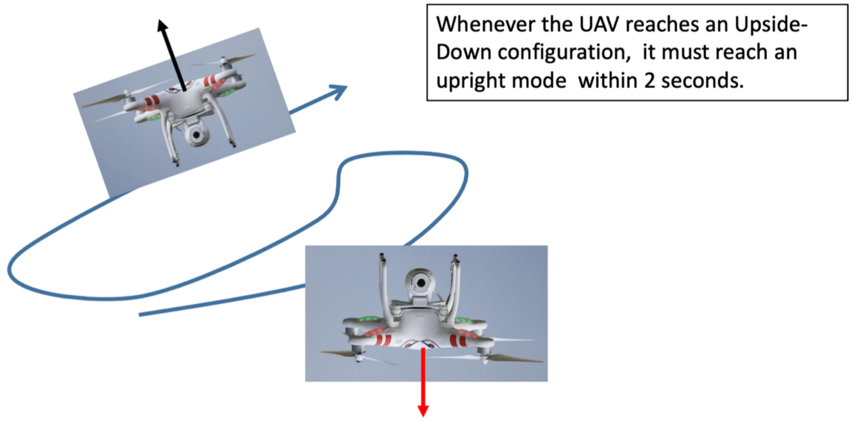
Rechability



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

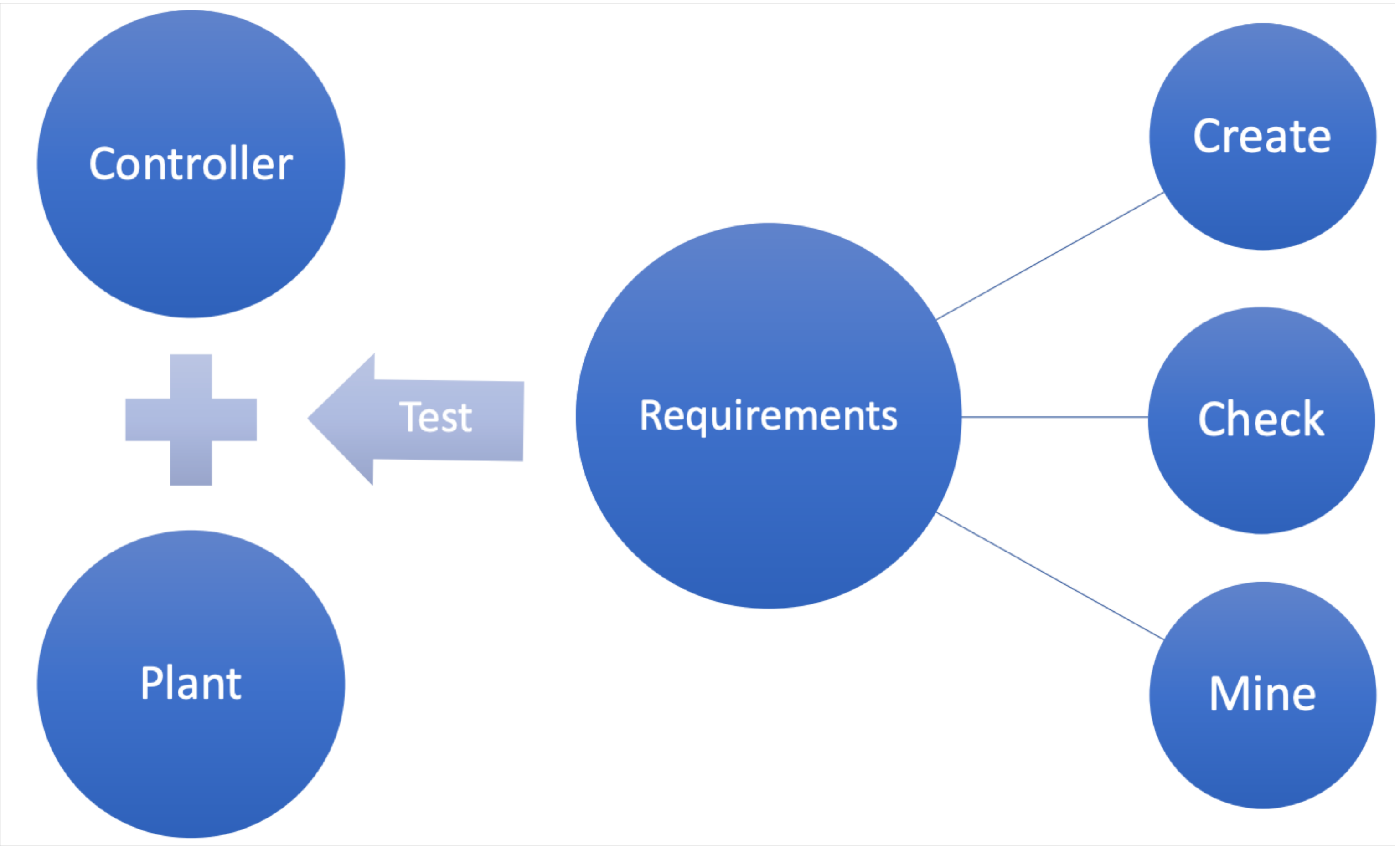
Mathematical, Algorithmic techniques for modeling, design, analysis

– **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

- Software Engineering: Writing checkable requirements and tests

- Reinforcement Learning for CPS Safety Engineering?

- Learn autonomous software stack through case studies in autonomy

Course Overview

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

2. **Modeling formalism**: Timed Automata, hybrid and switching systems, Markov Decision Process (MDP), Hidden Markov models, Partially observable MDP.

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

4. **Reinforcement Learning**: Bellman optimality equations and Dynamic Programming, Sequential Bayesian updating, Model-free learning, Stochastic optimization, Temporal difference learning, Critic-only, actor-only and actor-critic algorithms, Function approximation and generalization, Deep reinforcement learning.

Books

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

Grading

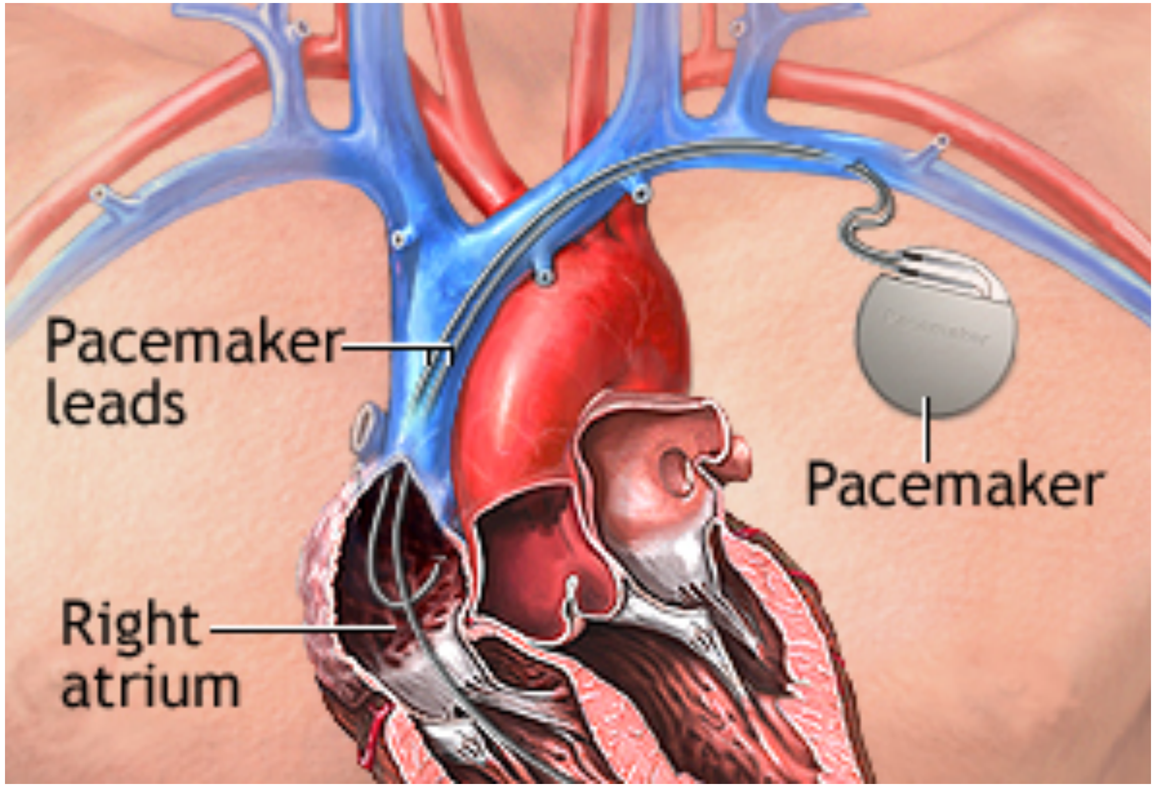
Project with a practice development of a CPS application, verification of formal requirements and falsification or test generation experiments

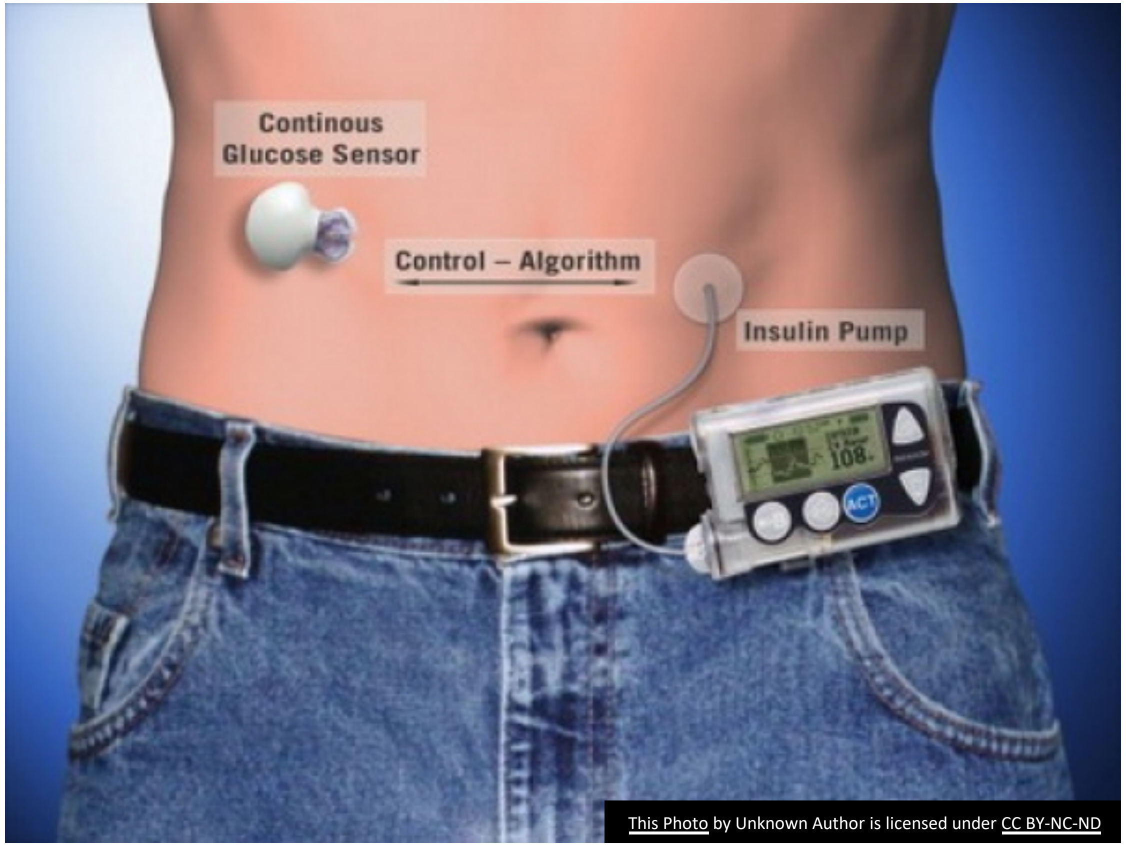
- Matlab/Simulink (simulation) model of a CPS application
- Can also develop model in Python or Java if that is the preferred language (will require additional work for handling requirements but I can help you!)
- Open to other software solution

Oral exam with presentation of the Project

Who are you?

Medical Device

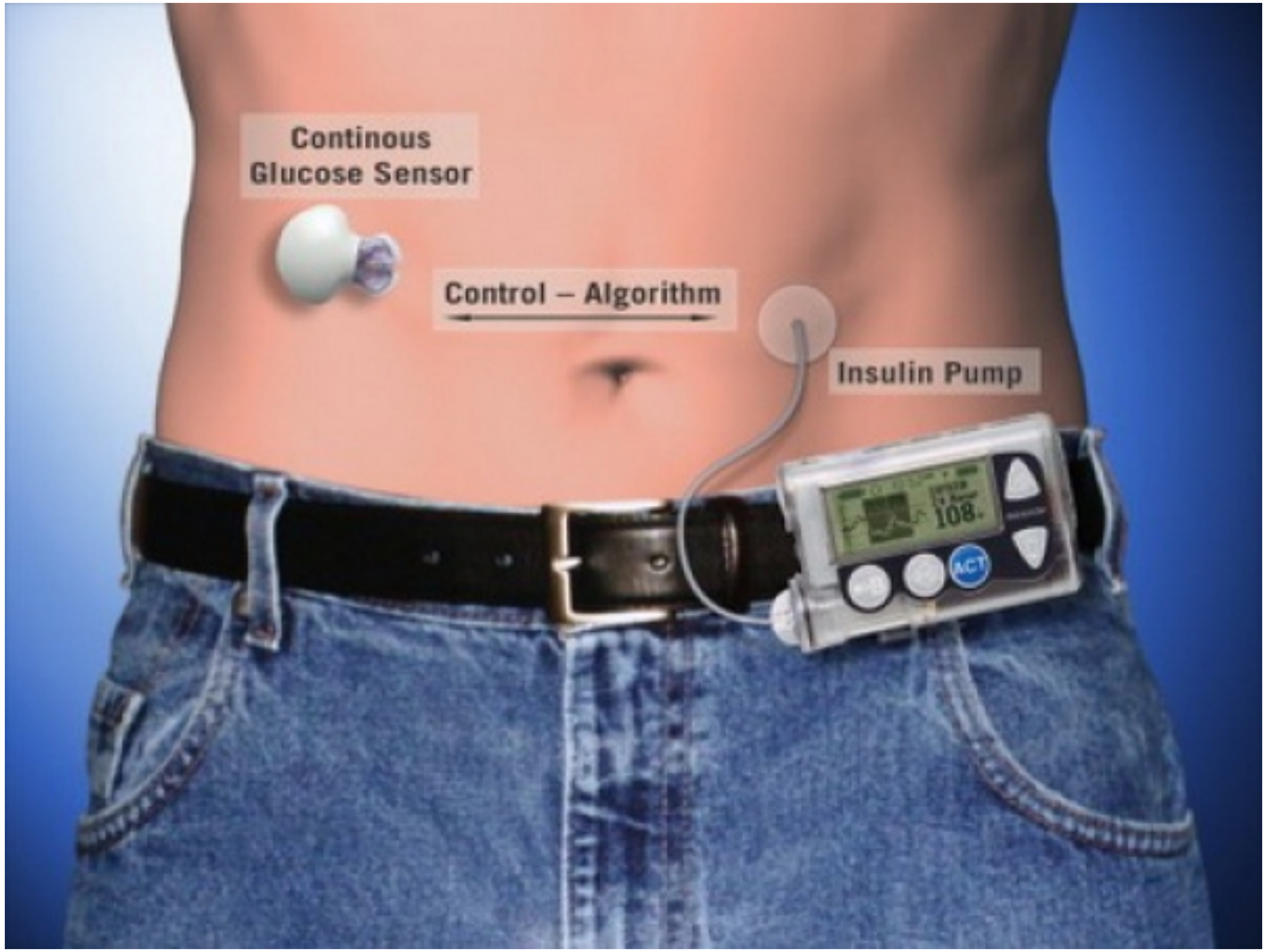




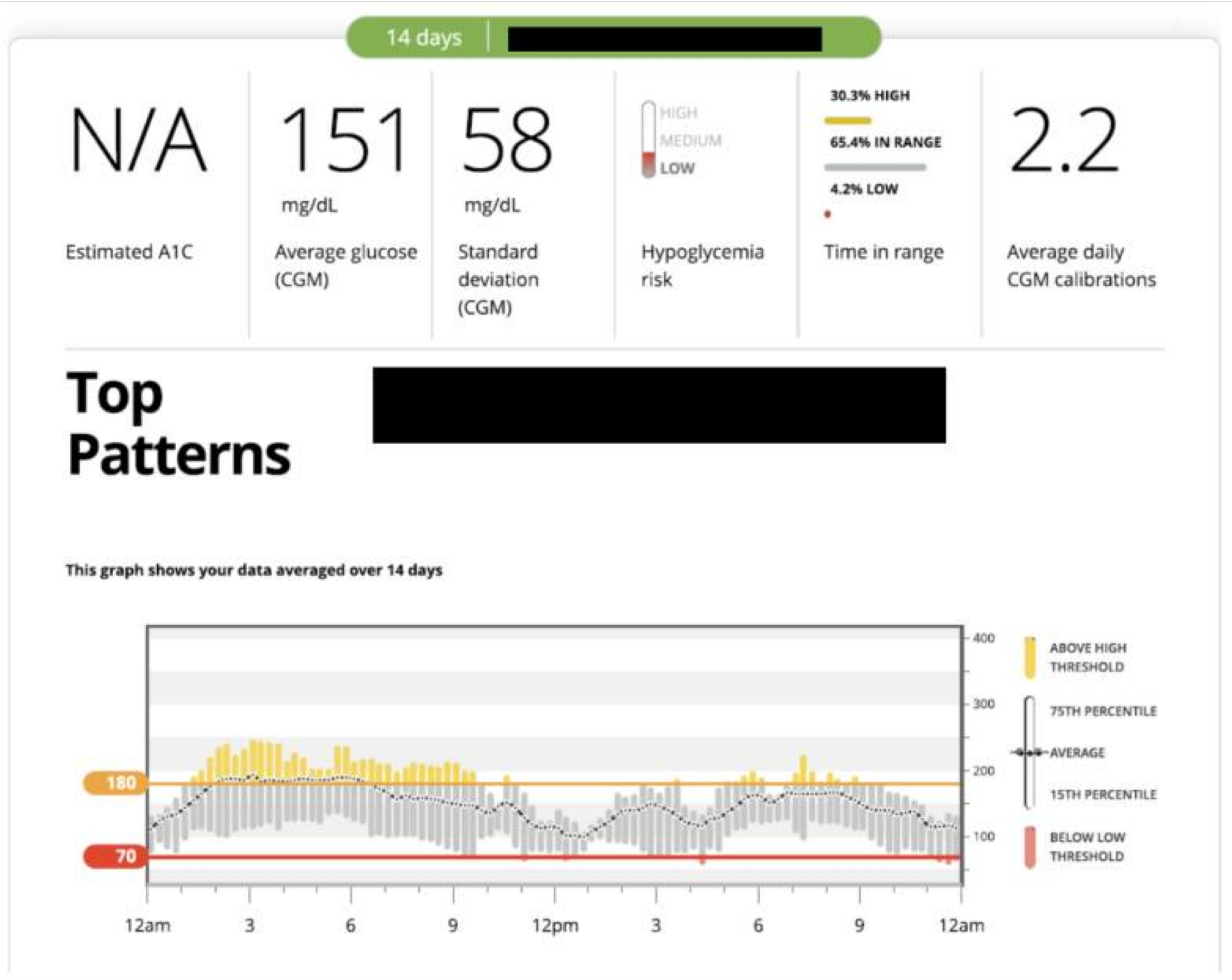
Artificial Pancreas

Type 1 diabetes occurs when the pancreas produces little or none of the insulin needed to regulate blood glucose

They rely on external administration of insulin to manage their blood glucose levels.



Continuous Glucose Monitoring



14 days | [redacted]

N/A

Estimated A1C

151 mg/dL

Average glucose (CGM)

58 mg/dL

Standard deviation (CGM)

HIGH
MEDIUM
LOW

Hypoglycemia risk

30.3% HIGH

65.4% IN RANGE

4.2% LOW

Time in range

2.2

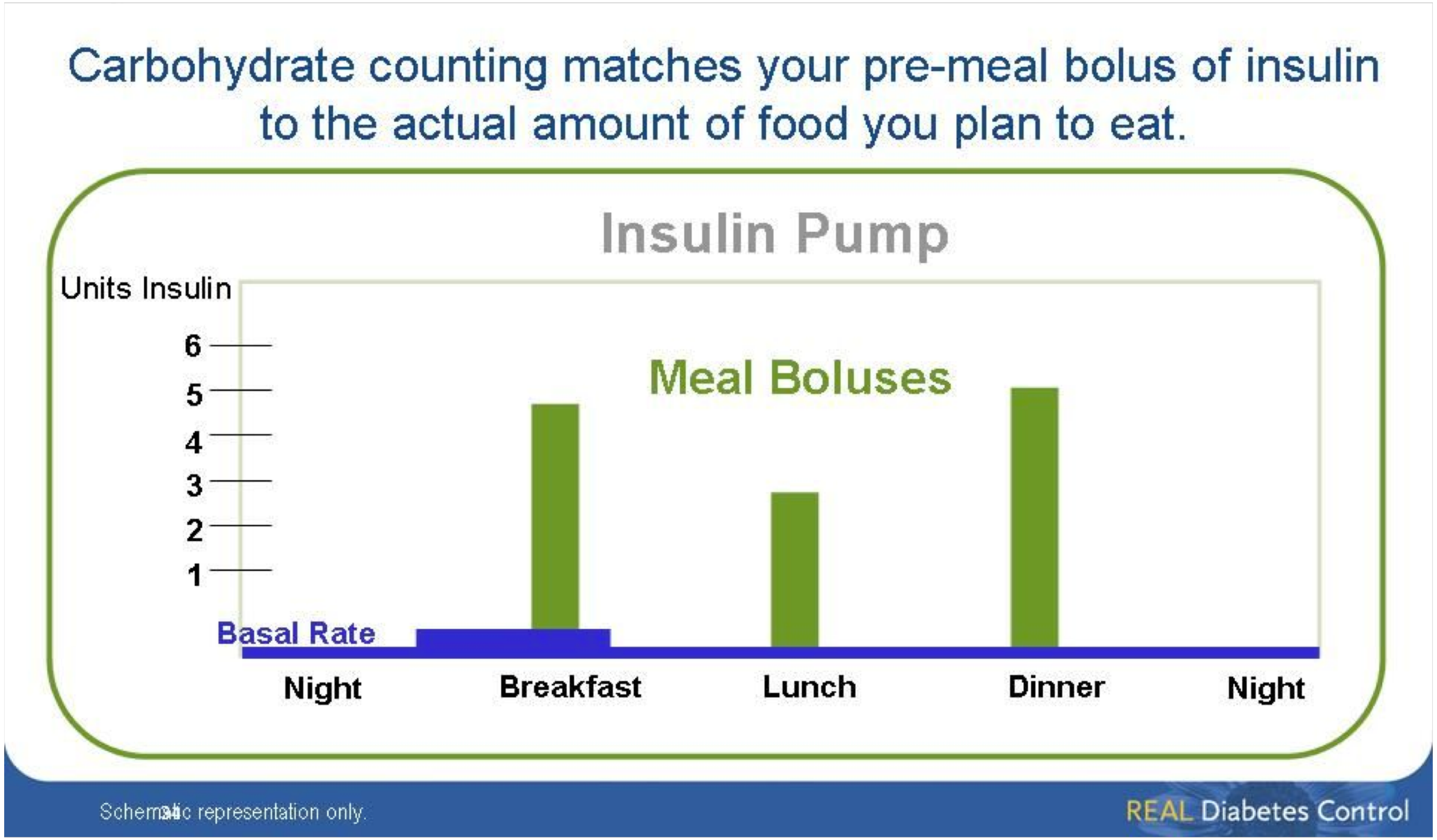
Average daily CGM calibrations

Top Patterns

[redacted]

This graph shows your data averaged over 14 days

Insulin pumps

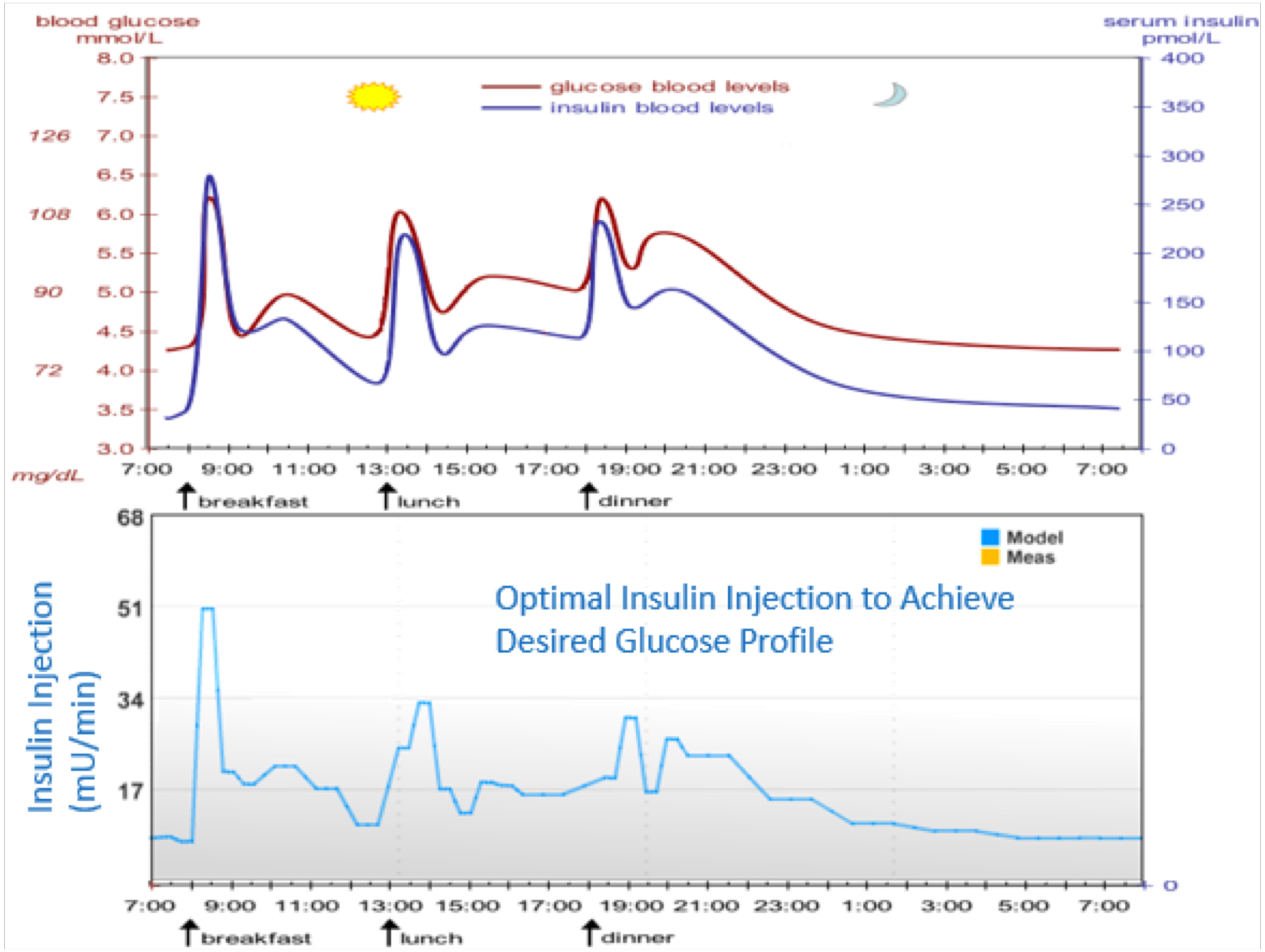


Carbohydrate counting matches your pre-meal bolus of insulin to the actual amount of food you plan to eat.

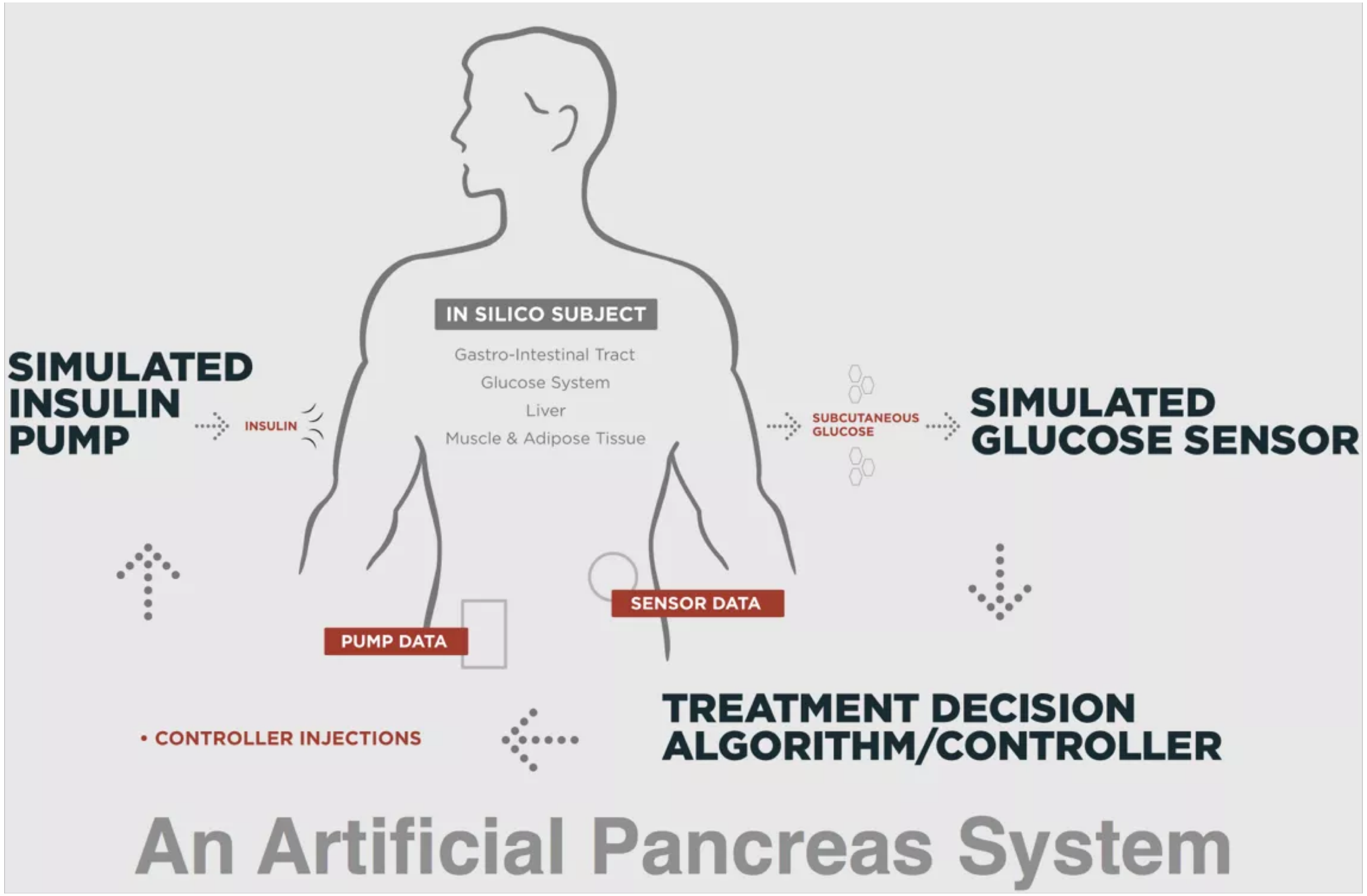
Schematic representation only.

REAL Diabetes Control

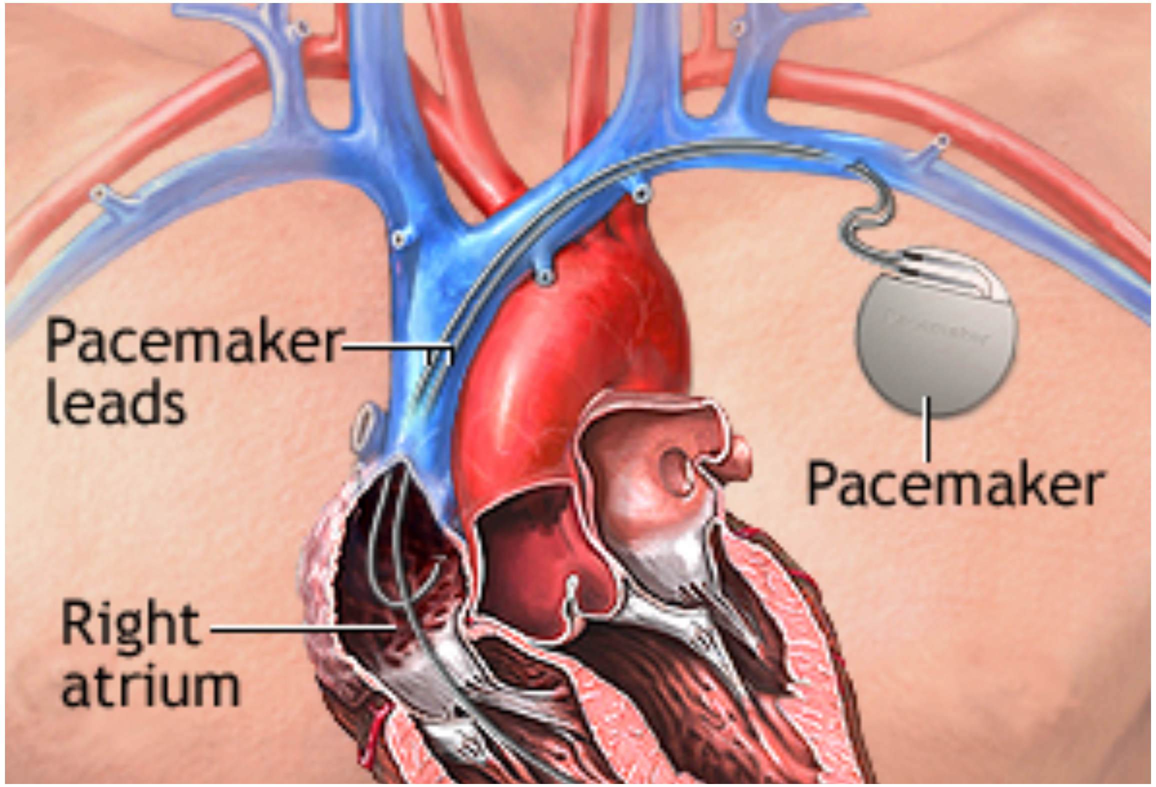
Artificial Pancreas


Optimal Insulin Injection to Achieve Desired Glucose Profile

Artificial Pancreas

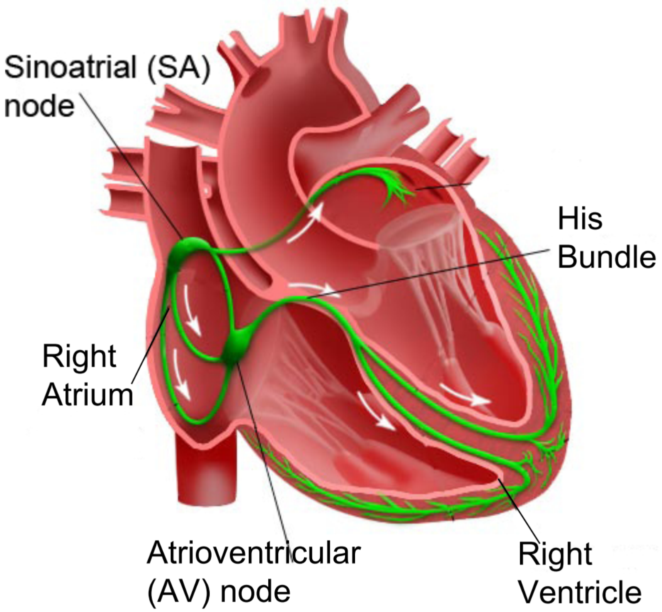


PaceMaker



Z. Jiang, M. Pajic, S. Moarref, R. Alur, R. Mangharam, *Modeling and Verification of a Dual Chamber Implantable Pacemaker*, In Proceedings of Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.

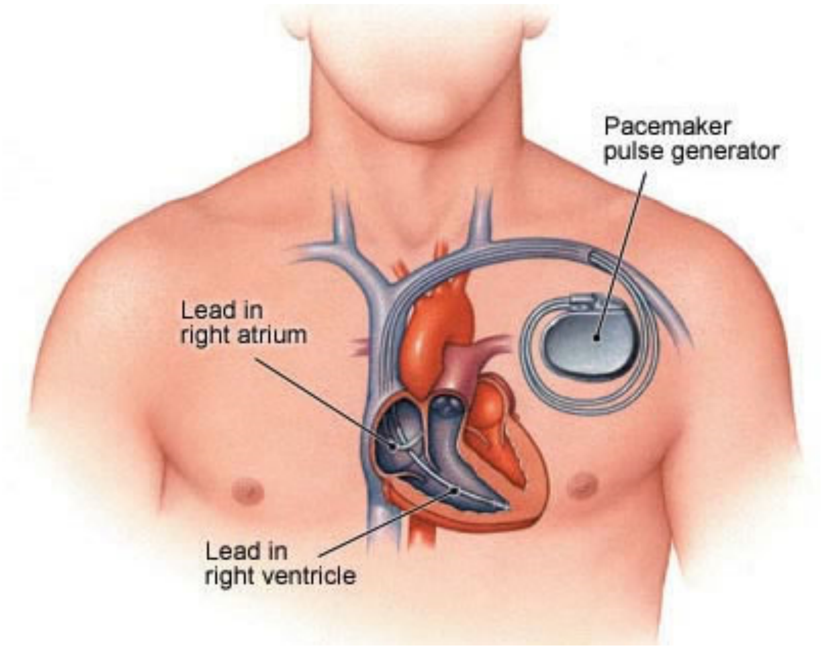
How does a healthy heart work?



- SA node (controlled by nervous system) periodically generates an electric pulse
- This pulse causes both atria to contract pushing blood into the ventricles
- Conduction is delayed at the AV node allowing ventricles to fill
- Finally the His-Pukinje system spreads electric activation through ventricles causing them both to contract, pumping blood out of the heart

Z. Jiang, M. Pajic, S. Moarref, R. Alur, R. Mangharam, *Modeling and Verification of a Dual Chamber Implantable Pacemaker*, In Proceedings of Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.

PaceMaker

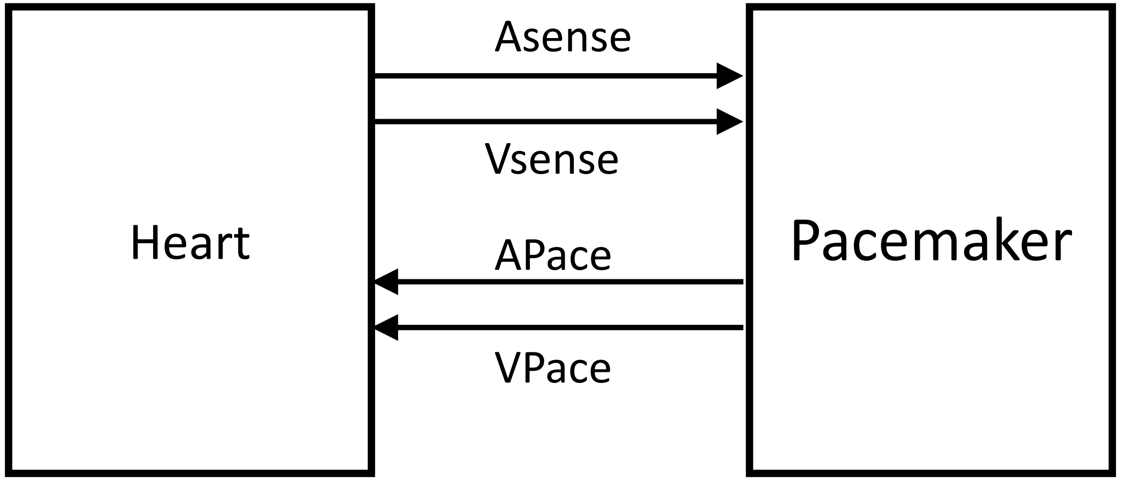


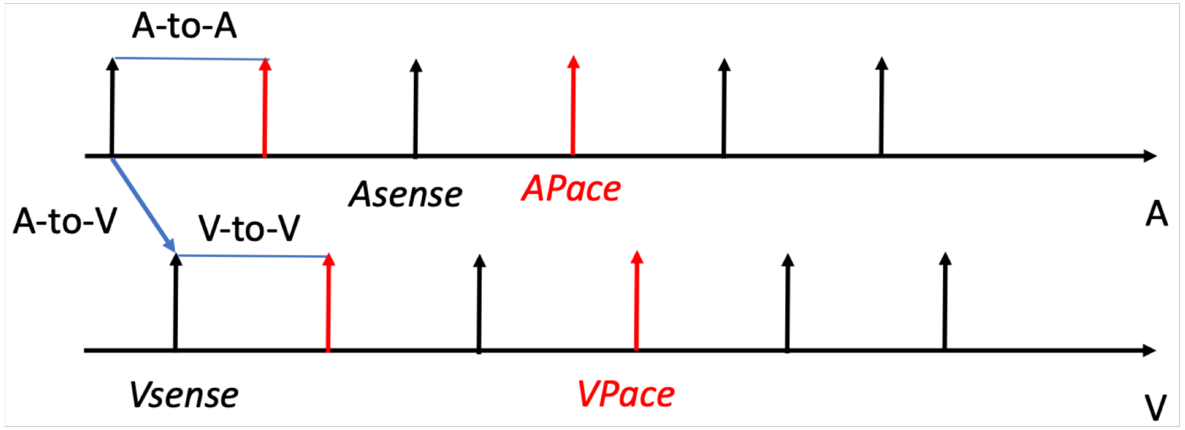
- Aging and/or diseases cause conduction properties of heart tissue to change leading to changes in heart rhythm
- Tachycardia: faster than desirable heart rate impairing hemo-dynamics (blood flow dynamics)
- Bradycardia: slower heart rate leading to insufficient blood supply
- Pacemakers can be used to treat bradycardia by providing pulses when heart rate is low

How dual-chamber pacemakers work

- Activation of local tissue sensed by the leads (giving rise to events Atrial Sense and Ventricular Sense)

- Atrial Pace or Ventricular Pace are delivered if no sensed events occur within deadlines

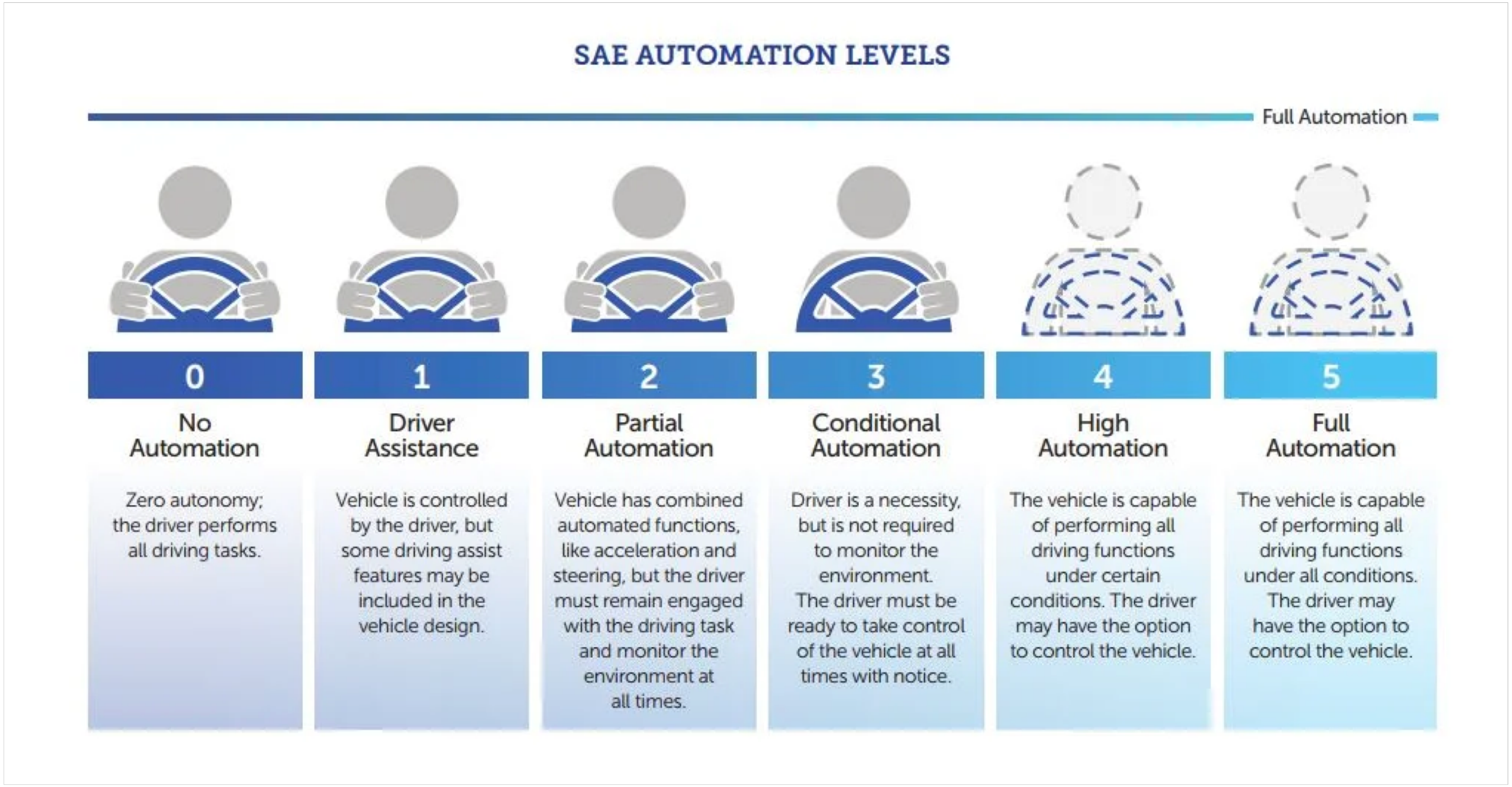




Transportation CPS

Everything that moves will become autonomous

Automotive Car

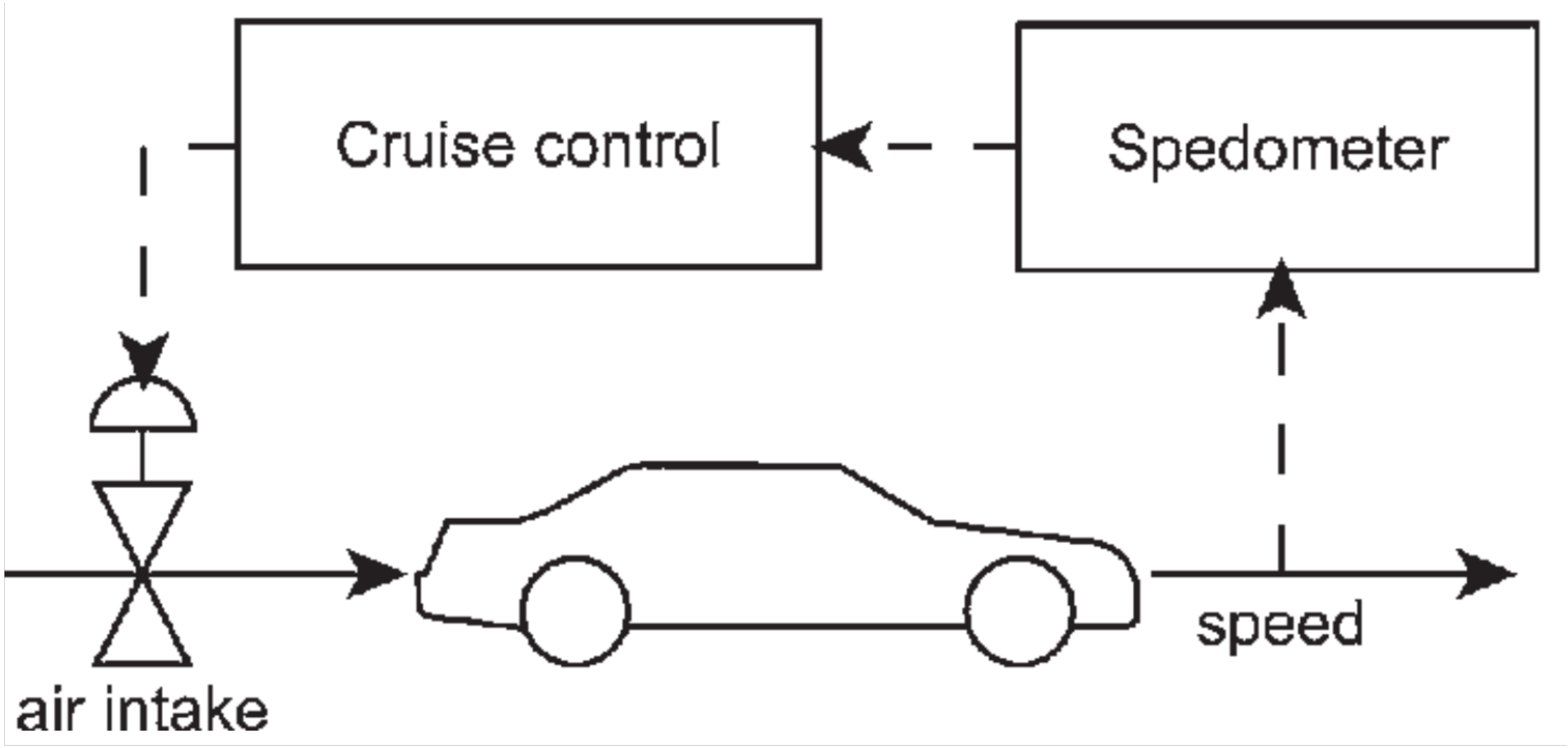


SAE AUTOMATION LEVELS

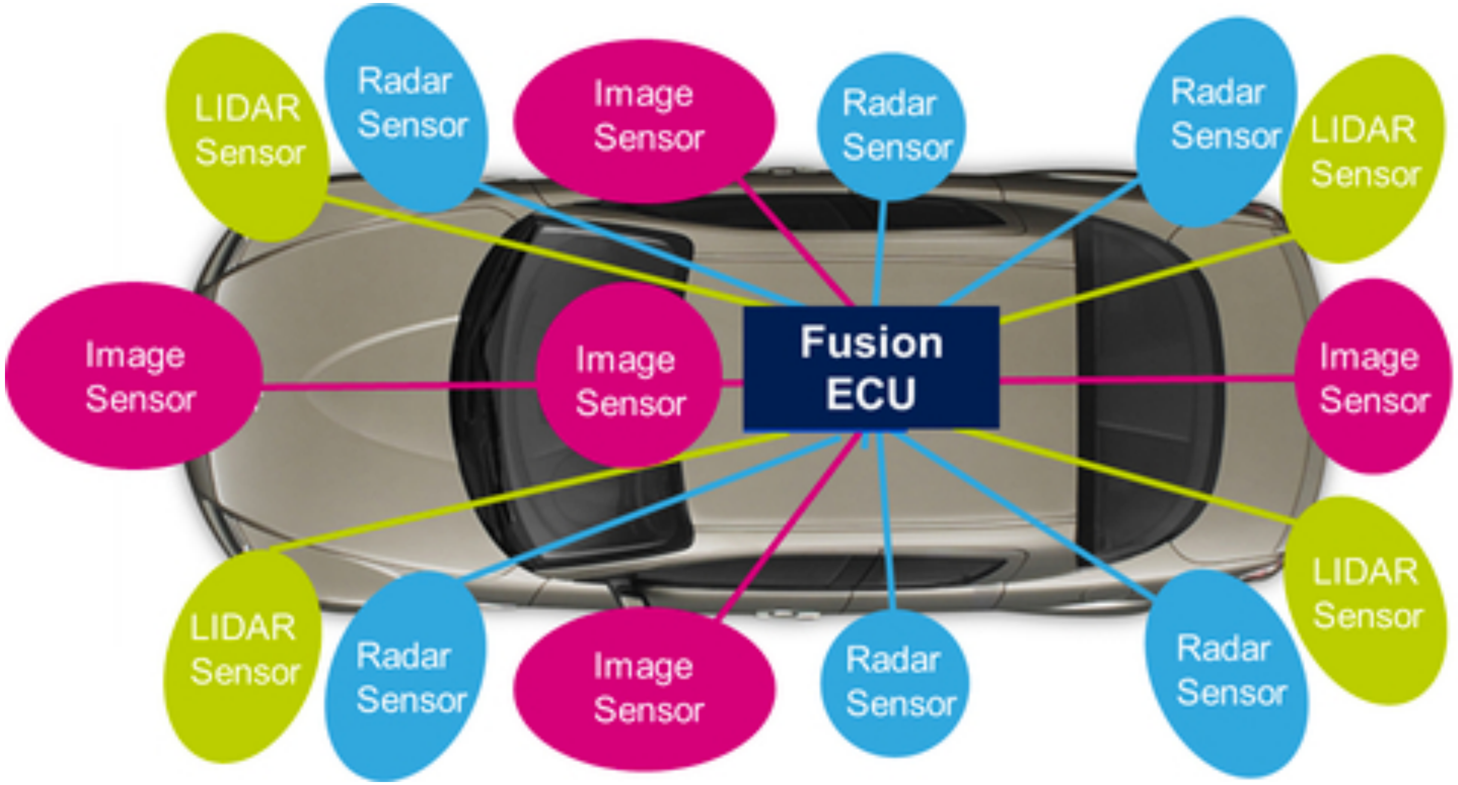
Full Automation

0	1	2	3	4	5
No Automation	Driver Assistance	Partial Automation	Conditional Automation	High Automation	Full Automation
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

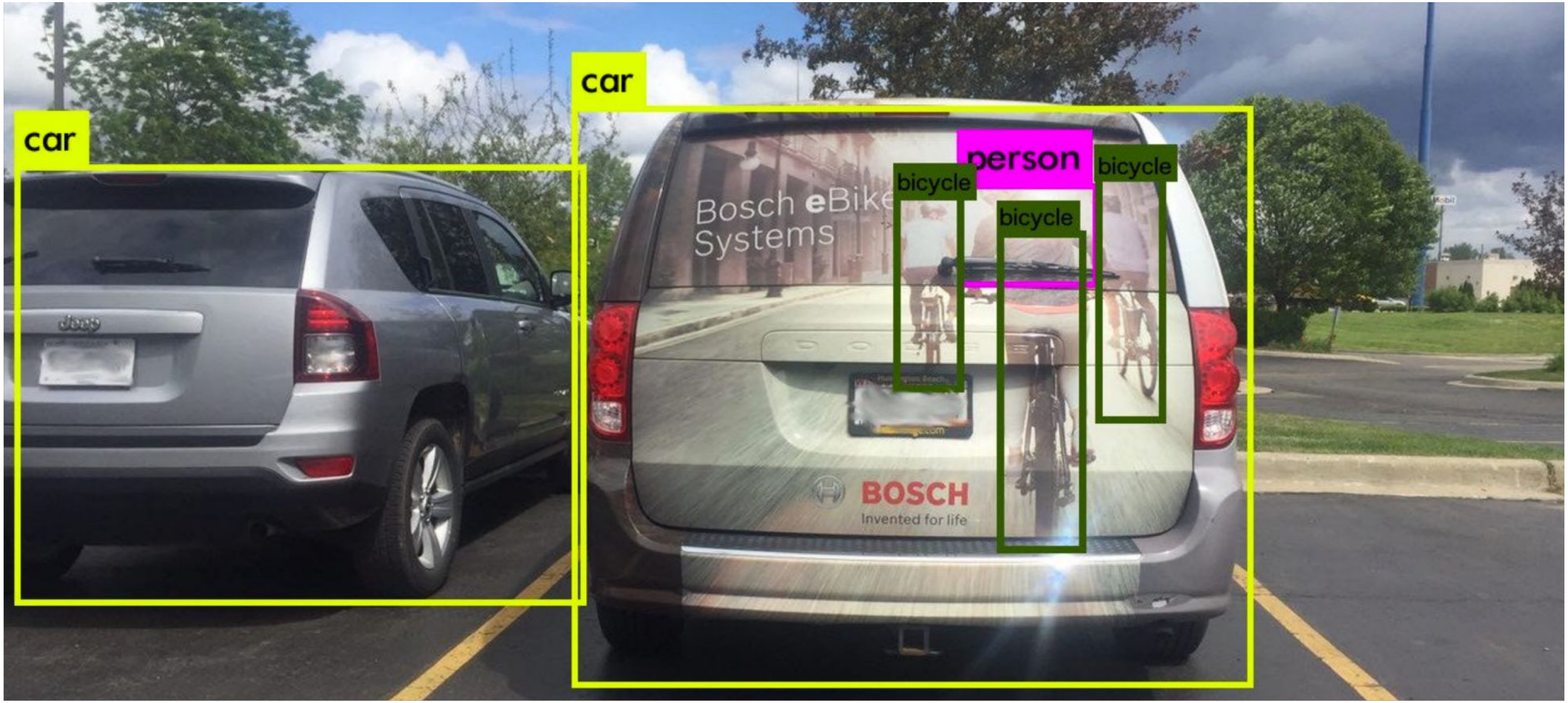
Automotive Car



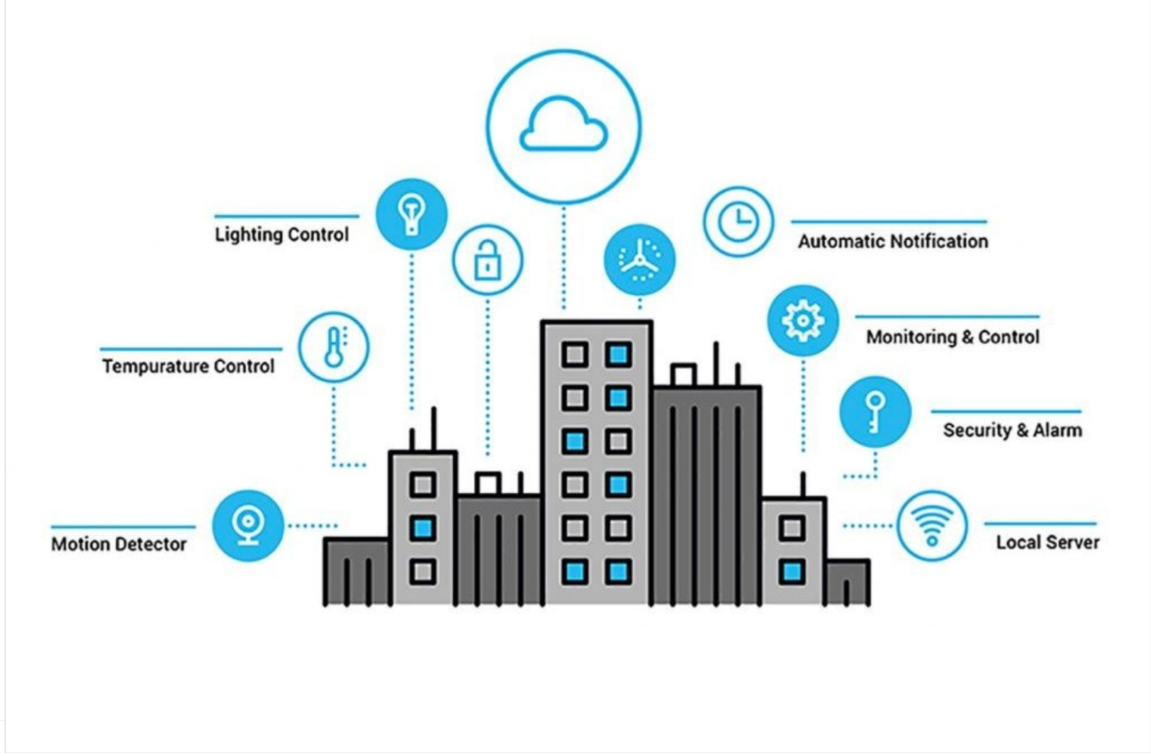
Automotive Car

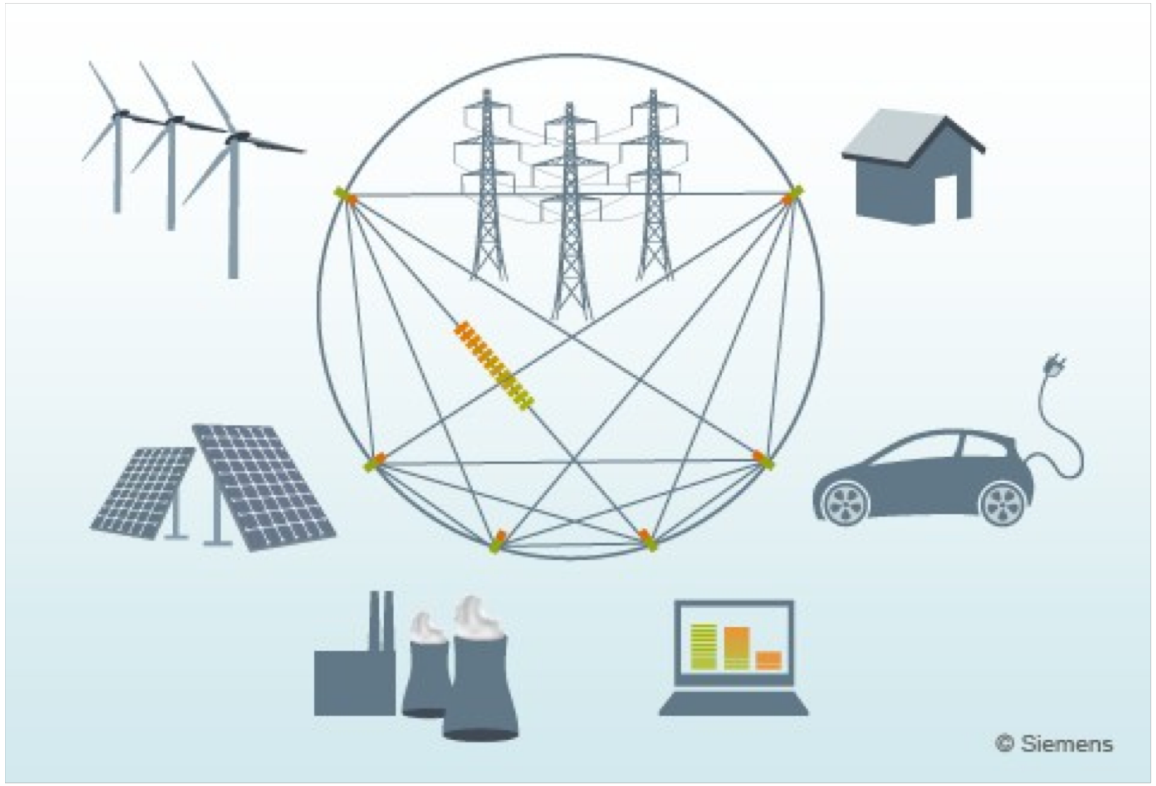


Automotive Car

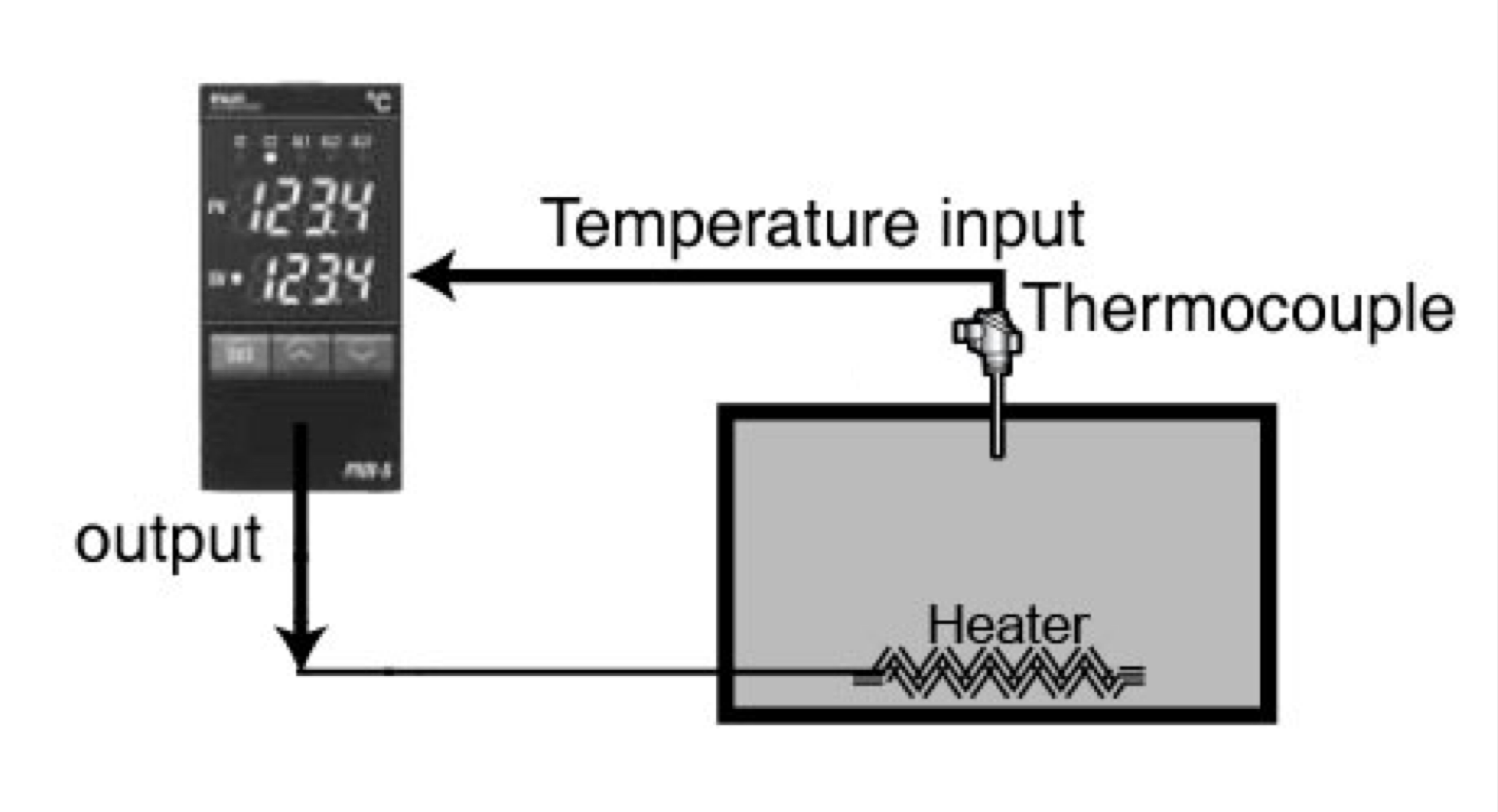


Energy

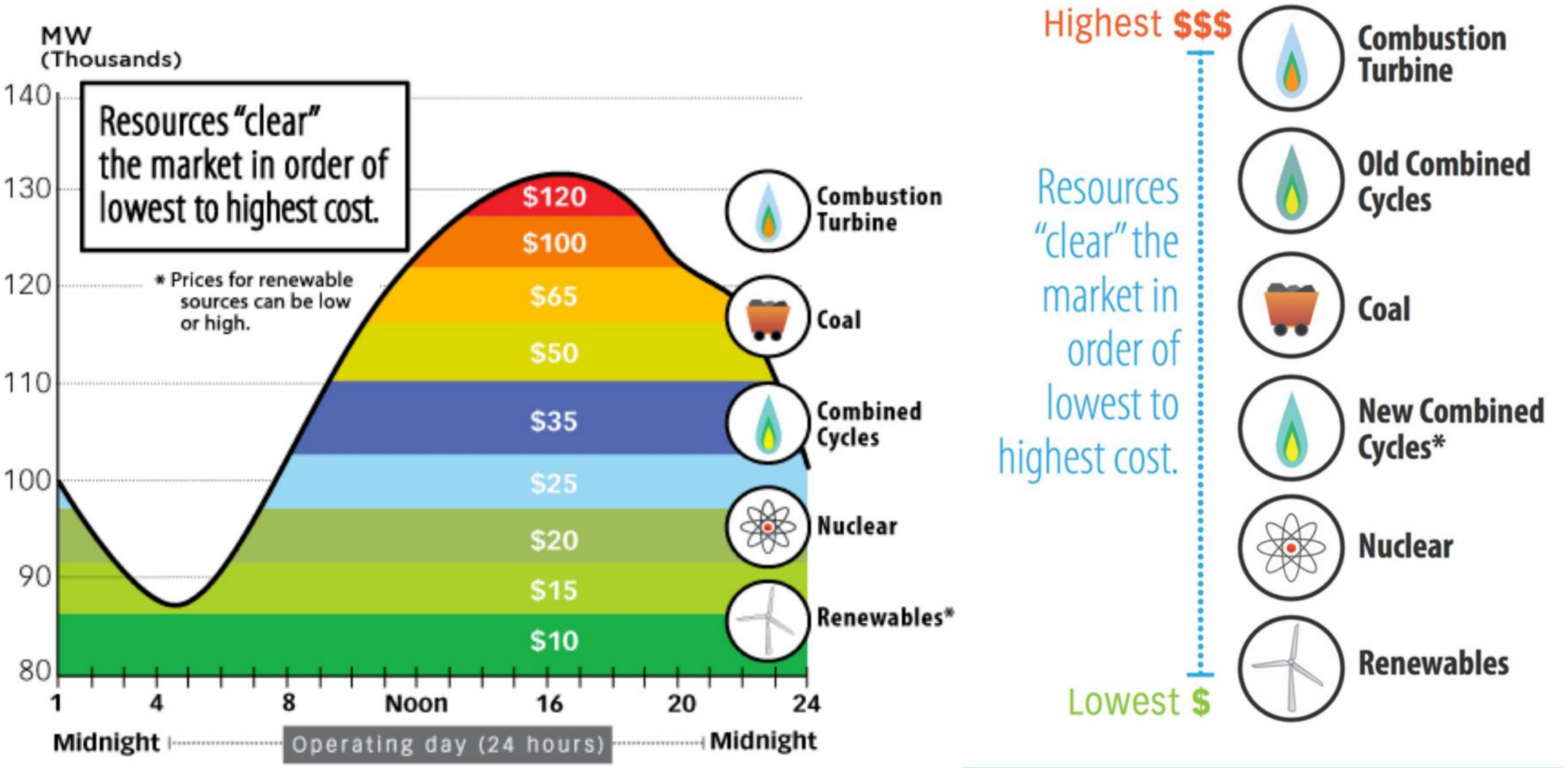



© Siemens

Temperature Control



Energy Control


MW
(Thousands)
140
130
120
110
100
90
80
Resources "clear" the market in order of lowest to highest cost.
* Prices for renewable sources can be low or high.
$120
$100
$65
$50
$35
$25
$20
$15
$10
1
4
8
Noon
16
20
24
Midnight
Operating day (24 hours)
Midnight
Combustion Turbine
Coal
Combined Cycles
Nuclear
Renewables*
Highest $$$
Resources "clear" the market in order of lowest to highest cost.
Lowest $
Combustion Turbine
Old Combined Cycles
Coal
New Combined Cycles*
Nuclear
Renewables