

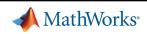


Model-Based Design of Next-Generation Cyber-Physical Systems

Akshay Rajhans, Ph.D.
Senior Research Scientist
MathWorks
<https://arajhans.github.io>

© 2017 The MathWorks, Inc.

About me



Research and Development
Application Engineering



MS
Research Staff



BOSCH Research Intern

Carnegie Mellon PhD



Advanced Research & Technology Office

- Research Community Engagement
- Tech Transfer
- Computational Content Creation
- Tech Knowledge Communication
- IP Cultivation
- Contributing to Research Strategy

Outline

- What's unique about cyber-physical systems (CPS)
- A CPS feature classification
- Challenges
- Opportunities

3

Tomorrow's systems are envisioned to be smart

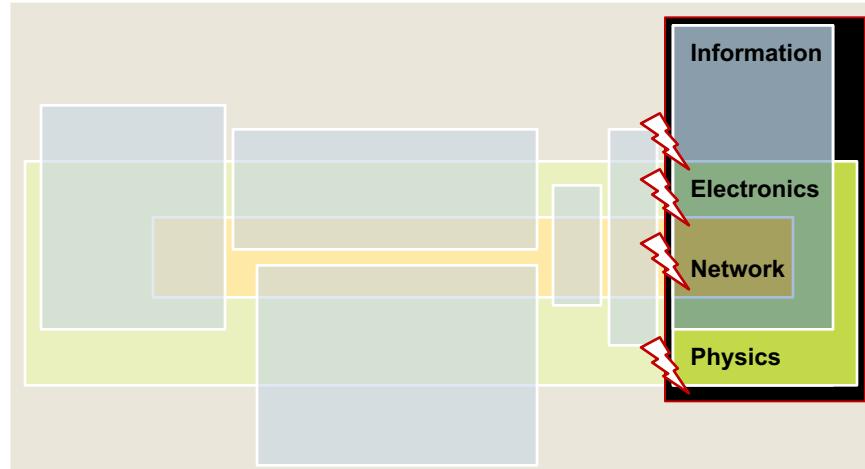
- Smart energy
- Smart mobility
- Smart health
- Smart manufacturing
- Smart cities

Q: How do we define, design,
and develop the smarts?

4

Networked embedded systems

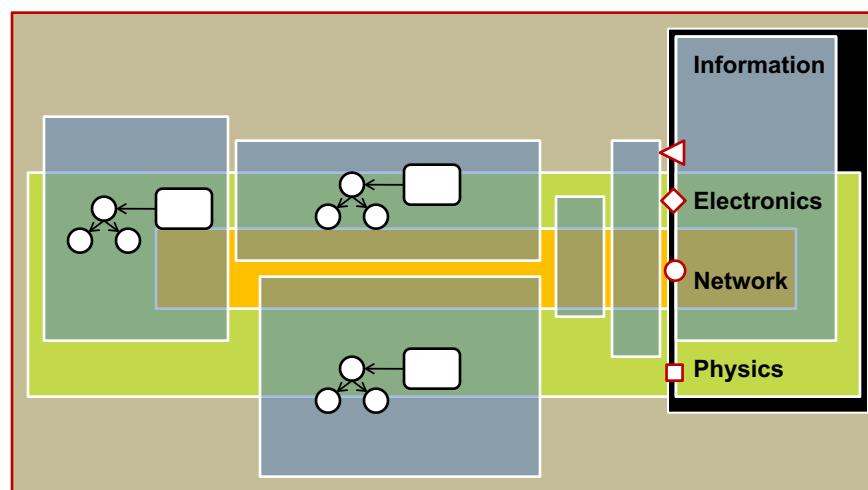
MathWorks®



5

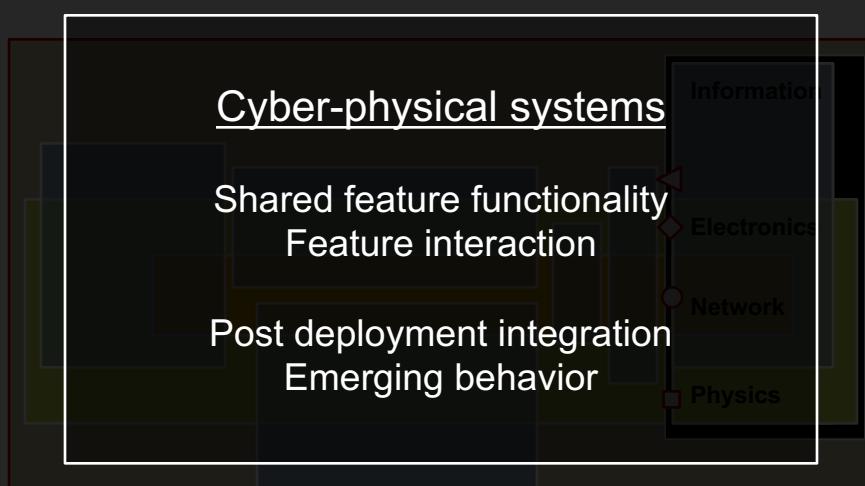
Cyber-physical systems

MathWorks®



6

Cyber-physical systems

A diagram illustrating the architecture of Cyber-physical systems. It shows four nested layers: Information, Electronic, Network, and Physics. Arrows point from the center of each layer to a central box containing the text "Cyber-physical systems". Below this, two more boxes contain "Shared feature functionality" and "Feature interaction" on top, and "Post deployment integration" and "Emerging behavior" on the bottom.

Cyber-physical systems

Shared feature functionality
Feature interaction

Post deployment integration
Emerging behavior

Information
Electronic
Network
Physics

7



A feature characterization for smart systems

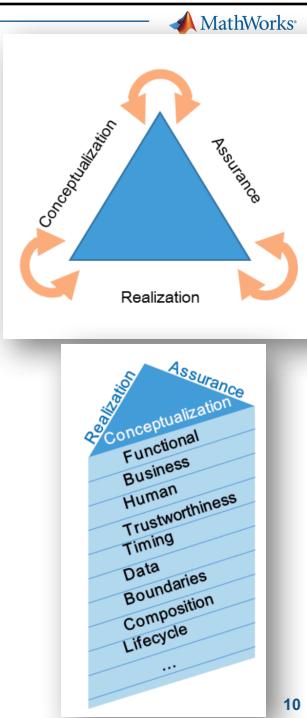
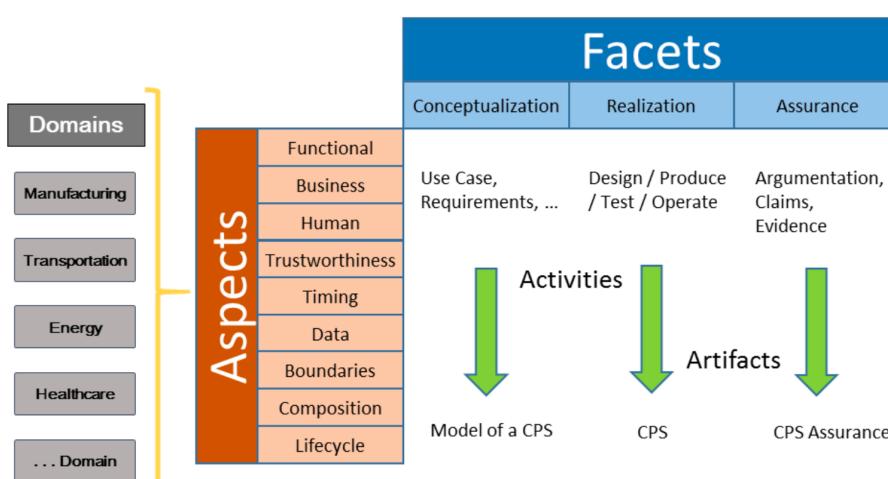
8

How do we characterize and develop ‘smartness’?

- Smart energy
- Smart mobility
- Smart health
- Smart manufacturing
- Smart cities

9

NIST CPS Framework – Facets



<https://pages.nist.gov/cpspwg/>

10

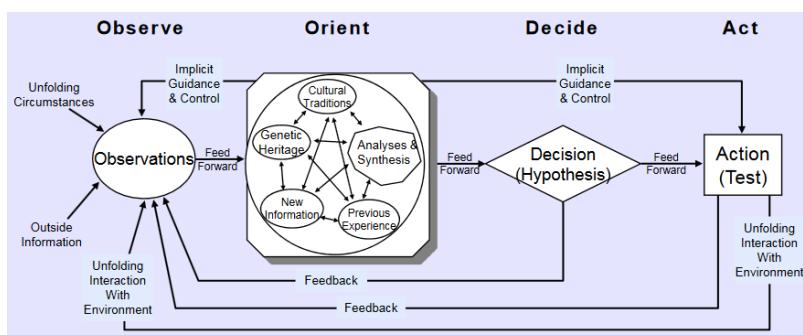
How do we characterize and develop smarts?

- Smart energy
- Smart mobility
- Smart health
- Smart manufacturing
- Smart cities

Q: How do we define, design, and develop smarts?

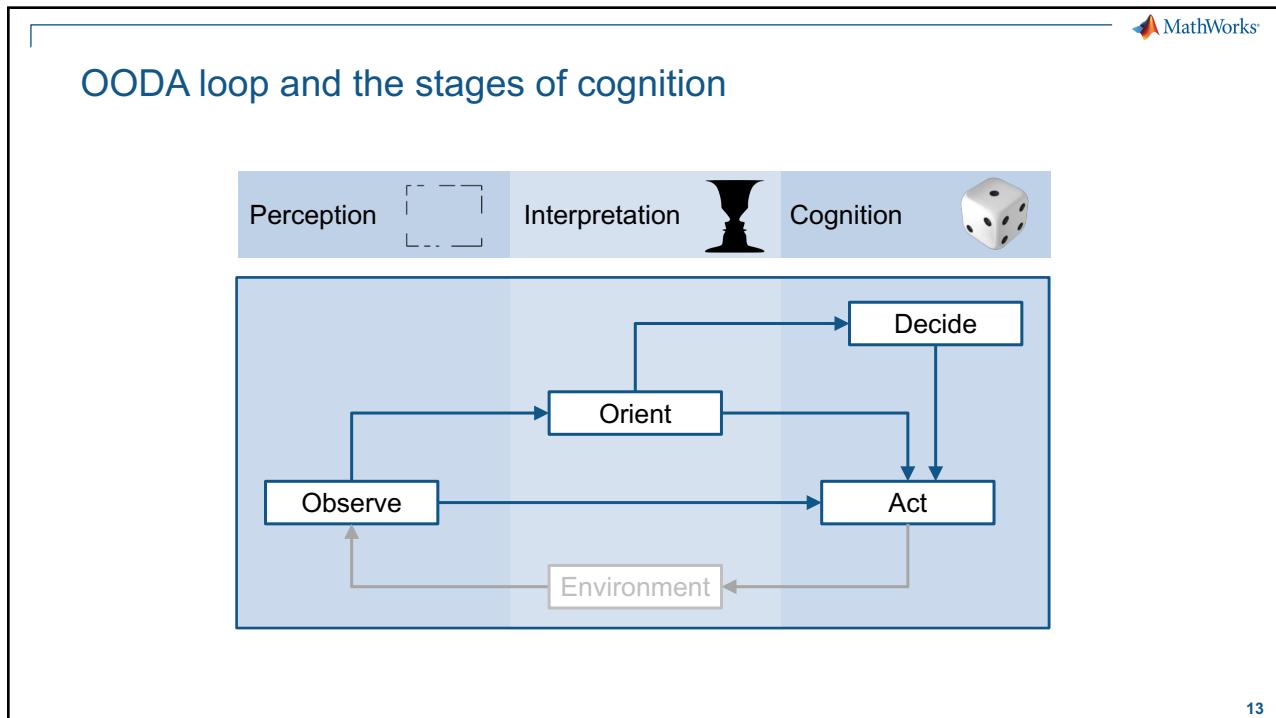
11

The Observe-Orient-Decide-Act (OODA) loop

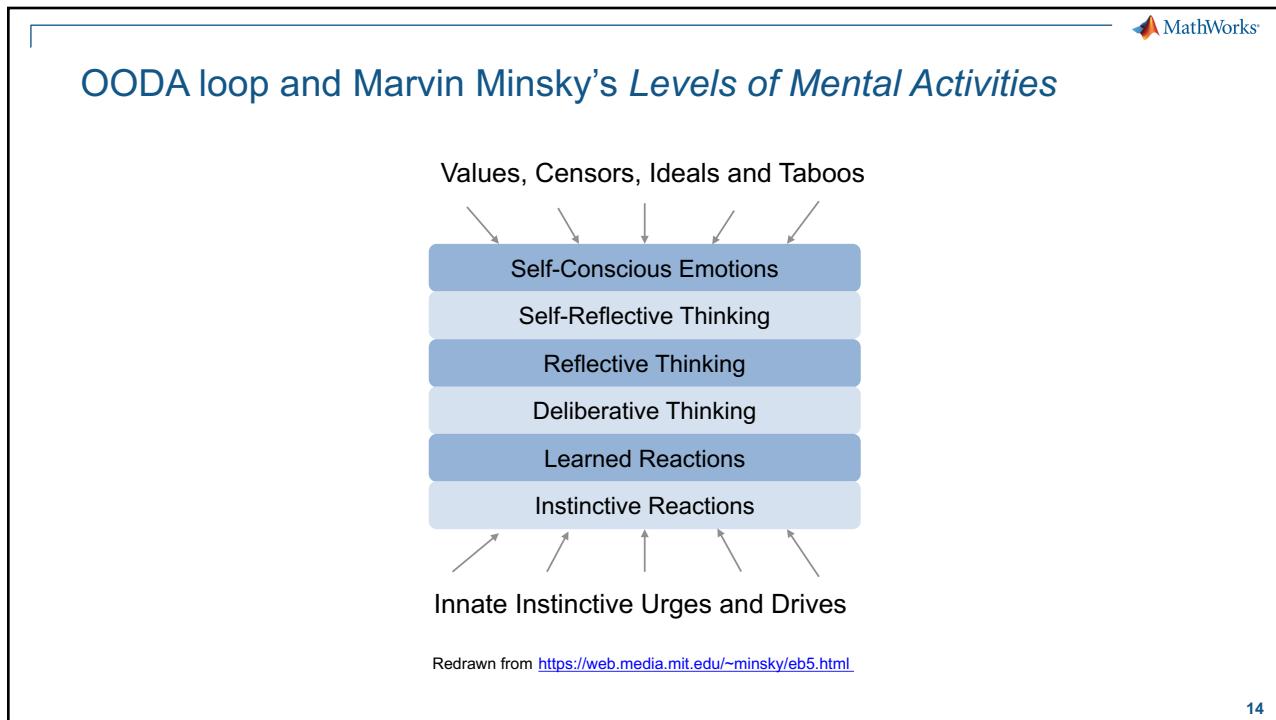


[https://en.wikipedia.org/wiki/John_Boyd_\(military_strategist\)#The_OODA_Loop](https://en.wikipedia.org/wiki/John_Boyd_(military_strategist)#The_OODA_Loop)

12

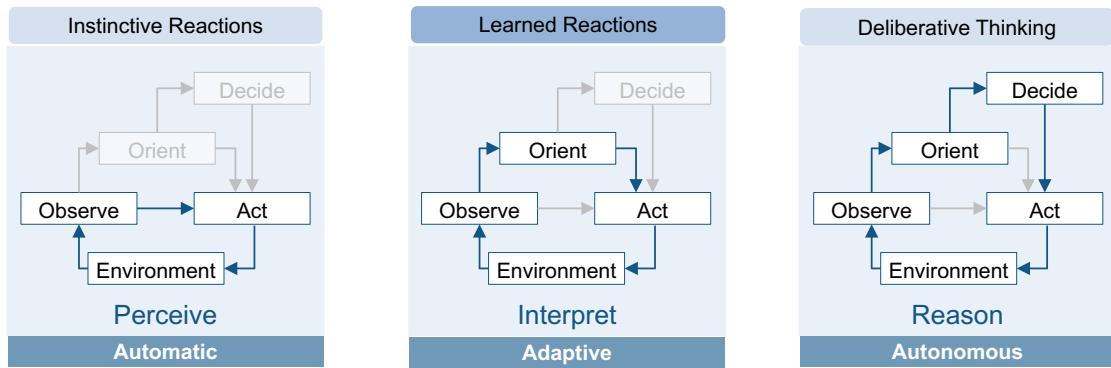


13



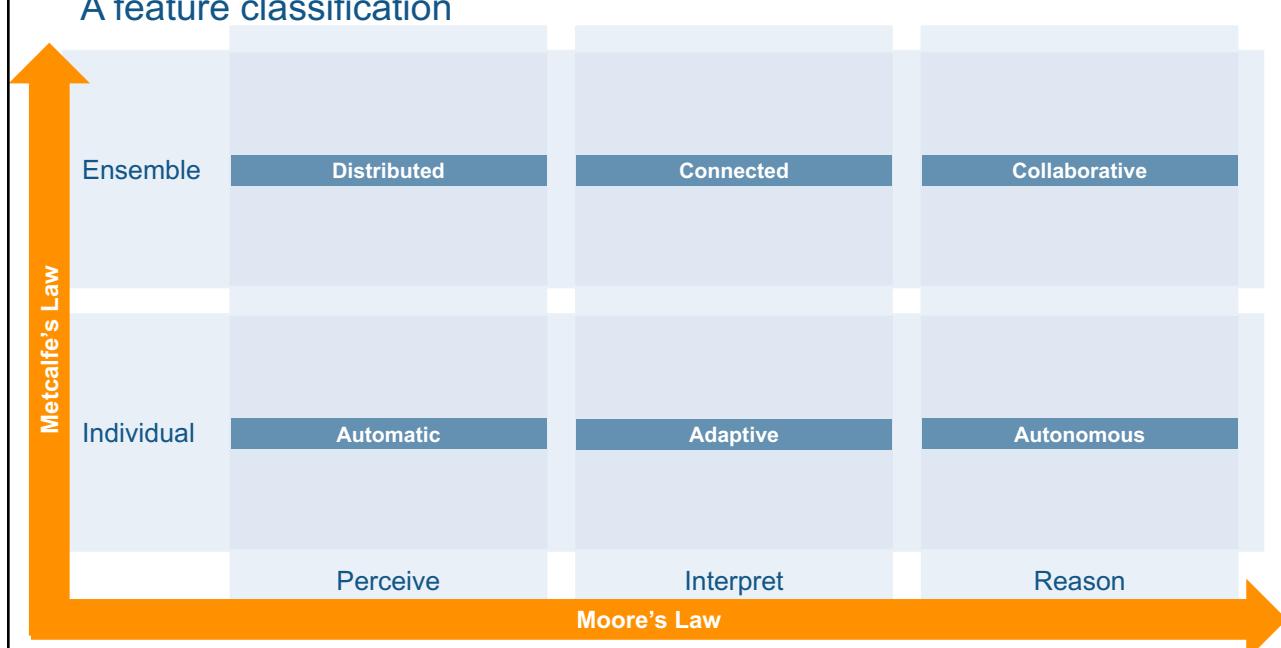
14

A feature classification



15

A feature classification





Adaptive

Conceptualize

- How to limit learning to safe behavior?

Realize

- What sensory system has sufficient richness?
 - How to prevent over interpretation?
- Robustness against interpretation edge case?
- Correctly fuse sensor data that is misaligned in time and space?

Assure

- How to test a self-changing artifact?
 - If regimes are not pre enumerated?
- Ensure successful and correct online calibration?

Twitter taught Microsoft's AI chatbot to be a racist a hole in less than a day

By James Vincent @jamesvinct Mar 24, 2016 6:36

68 comments



<https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>

Unfortunately, in the first 24 hours of coming online, a coordinated attack by a subset of people exploited a vulnerability in Tay. Although we had prepared for many types of abuses of the system, we had made a critical oversight for this specific attack.”

<http://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction>

17



Adaptive

Conceptualize

- How to limit learning to safe behavior?

Realize

- What sensory system has sufficient richness?
 - How to prevent over interpretation?
- Robustness against interpretation edge case?
- Correctly fuse sensor data that is misaligned in time and space?

Assure

- How to test a self-changing artifact?
 - If regimes are not pre enumerated?
- Ensure successful and correct online calibration?



Credit: Andre Penner/AP

“Father of the Internet: ‘AI stands for Artificial Idiot’ ”

<https://cacm.acm.org/news/217198-father-of-the-internet-ai-stands-for-artificial-idiot/fulltext>

18



Autonomous

Conceptualize

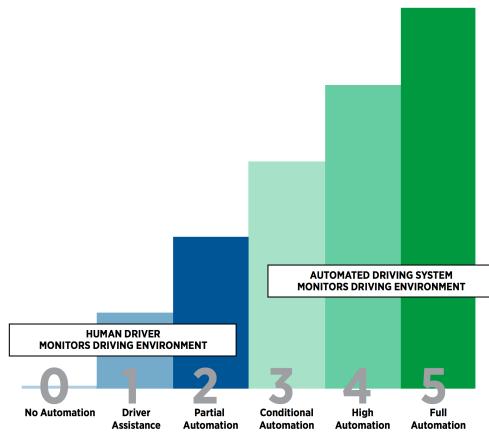
- Models of environment with sufficient predictive quality?
- Safe but nontrivial interaction with humans?
 - What are safe level of aggressiveness?

Realize

- Robust operation in an exceedingly complex environment?
- Fail safely with loss of minimum information?
- Know a planned action is safe?
- Assess risk online?

Assure

- Turing test for cars?
- Ensure the reasoning is always safe?
- Degraded safety (there is no perfect safety)?



SAE “levels of autonomy”

Learn more about SAE J3016 or purchase the standard document: www.sae.org/autodrive

https://www.sae.org/misc/pdfs/automated_driving.pdf



Connected

Conceptualize

- How to interpret data safely
 - Which data to corroborate information?

Realize

- Safely operate in the face of communication challenges
 - Degradation, loss
 - Corruption
- Timeliness and responsiveness guarantees?
 - Service discovery time out, DoS

Assure

- Is closed loop verification possible?
- How do you obtain failure probabilities?



the woman was following a route on her car's GPS while **driving in the dark on a foggy night** in Ontario when it directed her to drive onto a boat launch, and she ended up in a lake.

<http://www.news.com.au/technology/gadgets/woman-follows-gps-into-lake/news-story/a7d362dfc4634fd094651afc63f853a1>



Connected

Conceptualize

- How to interpret data safely
 - Which data to corroborate information?

Realize

- Safely operate in the face of communication challenges
 - Degradation, loss
 - Corruption
- Timeliness and responsiveness guarantees?
 - Service discovery time out, DoS

Assure

- Is closed loop verification possible?
- How do you obtain failure probabilities?



Tech issues cause most drone accidents: Research
Increased regulation and reporting of accidents needed for industry. Researchers
 RMIT UNIVERSITY

World-first research has found technical problems rather than operator errors are behind the majority of drone accidents, leading to a call for further safeguards for the industry.

Researchers Dr Graham Wild and Dr Glenn Baxter from RMIT University's School of Engineering, along with John Murray from Edith Cowan University, completed the first examination of more than 150 reported civil incidents around the world involving drones, or Remotely Piloted Aircraft Systems (RPAS).

The study showed technical problems were the cause of 64 per cent of the incidents, which occurred between ~2006 and 2016.

Recently published in the journal Aerospace, the study found that in most cases, **broken communications links** between the pilot and the Remotely Piloted Aircraft Systems (RPAS) were the cause of the incident,

https://www.eurekalert.org/pub_releases/2016-08/rutic082216.php

21



Connected

Conceptualize

- How to interpret data safely
 - Which data to corroborate information?

Realize

- Safely operate in the face of communication challenges
 - Degradation, loss
 - Corruption
- Timeliness and responsiveness guarantees?
 - Service discovery time out, DoS

Assure

- Is closed loop verification possible?
- How do you obtain failure probabilities?



MIT Technology Review
The Download

New Cyberattack Could Take Out Solar Arrays

Renewable energy may have a cybersecurity problem. At the recent BlackHat security conference, researchers found that it was possible to hack into the software that controls many wind farms, and potentially **take the turbines hostage**. Now it looks like... [Read more](#)

SOURCE: BBC IMAGE CREDIT: JAMES MORAN / FLICKR

amonthago

“... demonstrated that it’s possible to **remotely take control of the inverters**.
 “... a malicious hacker that gained access to a solar array in this way could **alter the flow of electricity** in such a way as to **cause an outage**.”

<https://www.technologyreview.com/the-download/608588/new-cyberattack-could-take-out-solar-arrays/>

22



Connected

Conceptualize

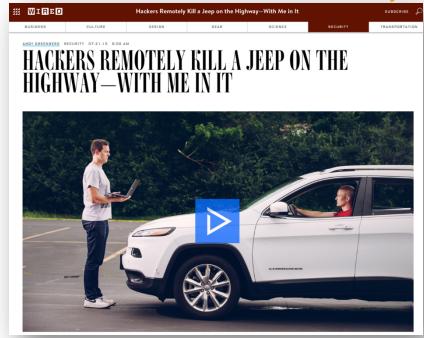
- How to interpret data safely
 - Which data to corroborate information?

Realize

- Safely operate in the face of communication challenges
 - Degradation, loss
 - Corruption
- Timeliness and responsiveness guarantees?
 - Service discovery time out, DoS

Assure

- Is closed loop verification possible?
- How do you obtain failure probabilities?



Hackers Remotely Kill a Jeep on the Highway—With Me In It

Uconnect's cellular connection also lets anyone who knows the car's IP address gain access from anywhere in the country.

From that entry point, the attack pivots to an adjacent chip [...] rewriting the firmware [...] capable of sending commands through the CAN bus, to its physical components like the engine and wheels.

<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>



Connected

Conceptualize

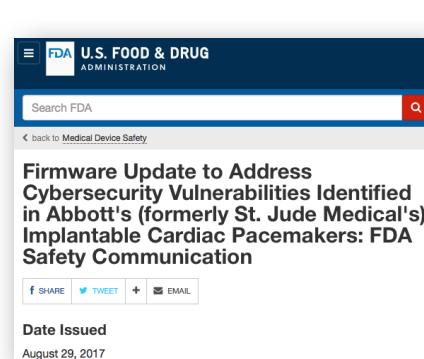
- How to interpret data safely
 - Which data to corroborate information?

Realize

- Safely operate in the face of communication challenges
 - Degradation, loss
 - Corruption
- Timeliness and responsiveness guarantees?
 - Service discovery time out, DoS

Assure

- Is closed loop verification possible?
- How do you obtain failure probabilities?



Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

Date Issued
August 29, 2017

“these vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment.

<https://www.fda.gov/MedicalDevices/SafetyandAlerts/AlertsandNotices/ucm573669.htm>



Collaborative

Conceptualize

- Cross-organization failure effect analysis?
- How to identify and prevent race conditions?
- Robust conflict resolution across an ensemble?
- How to trade off system vs. ensemble safety?

Realize

- Safety of ad hoc rules in collaboration?
- How to perform online safety analysis?
- How much risk to assign to a collaboration?
- How to gracefully enter/exit a collaboration?
- How to ensure ample resources to be safe?
- Can you assign probability to reliance?

Assure

- How do you test? Measure coverage?
- Work outside nominal regions (online derating)?
- Assumptions about collaborating systems?



Swiss regional air traffic chief Anton Maag said both aircraft were diving to avoid a crash when they flew into each other.

And he added that the Russian pilot had started a steep dive only after controllers had repeatedly instructed him to do so.

<http://news.bbc.co.uk/2/hi/europe/2082700.stm>

25



Collaborative

Conceptualize

- Cross-organization failure effect analysis?
- How to identify and prevent race conditions?
- Robust conflict resolution across an ensemble?
- How to trade off system vs. ensemble safety?

Realize

- Safety of ad hoc rules in collaboration?
- How to perform online safety analysis?
- How much risk to assign to a collaboration?
- How to gracefully enter/exit a collaboration?
- How to ensure ample resources to be safe?
- Can you assign probability to reliance?

Assure

- How do you test? Measure coverage?
- Work outside nominal regions (online derating)?
- Assumptions about collaborating systems?



The way humans often deal with these situations is that “they make eye contact. On the fly, they make agreements about who has the right of way,” said John Lee, a professor of industrial and systems engineering and expert in driver safety and automation at the University of Wisconsin.

<http://www.nytimes.com/2015/09/02/technology/personaltech/google-says-its-not-the-driverless-cars-fault-its-other-drivers.html>

26

Challenges

- **Scientific and technological challenges**
 - **Heterogeneity**: Multi-domain, multi-technology, multi-disciplinary nature
- **Socio-technical challenges**
 - **Trustworthiness**: safety, security, privacy, dependability
 - **Standardization and policy development**
 - Understanding **human interaction** with CPS
- **Education and workforce training challenges**
 - 21st century CPS education and workforce training

27

Research Questions

**Carnegie Mellon University
Research Showcase @ CMU**

Dissertations

Theses and Dissertations

5-2013

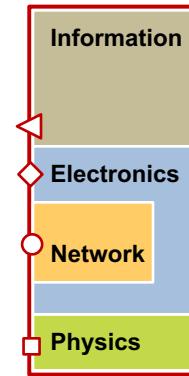
Multi-Model Heterogeneous Verification of Cyber-Physical Systems

Akshay H. Rajhans
Carnegie Mellon University

28

Design of heterogeneous systems

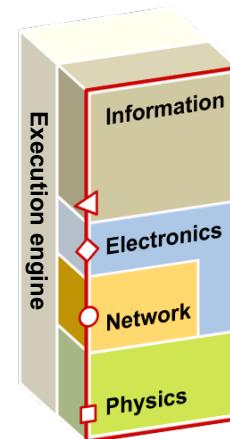
- Executable models
 - Quick feedback on design options
 - Automate design tasks
 - Automate synthesis tasks
 - ...
- Computational semantics



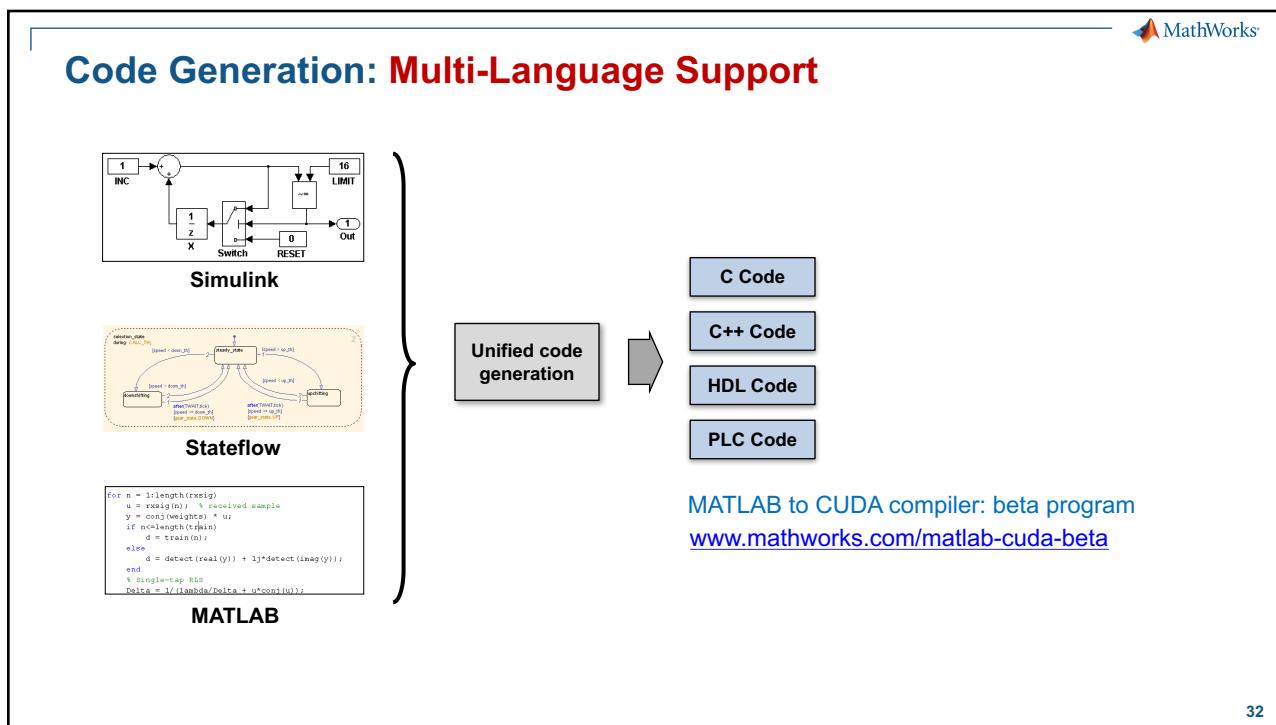
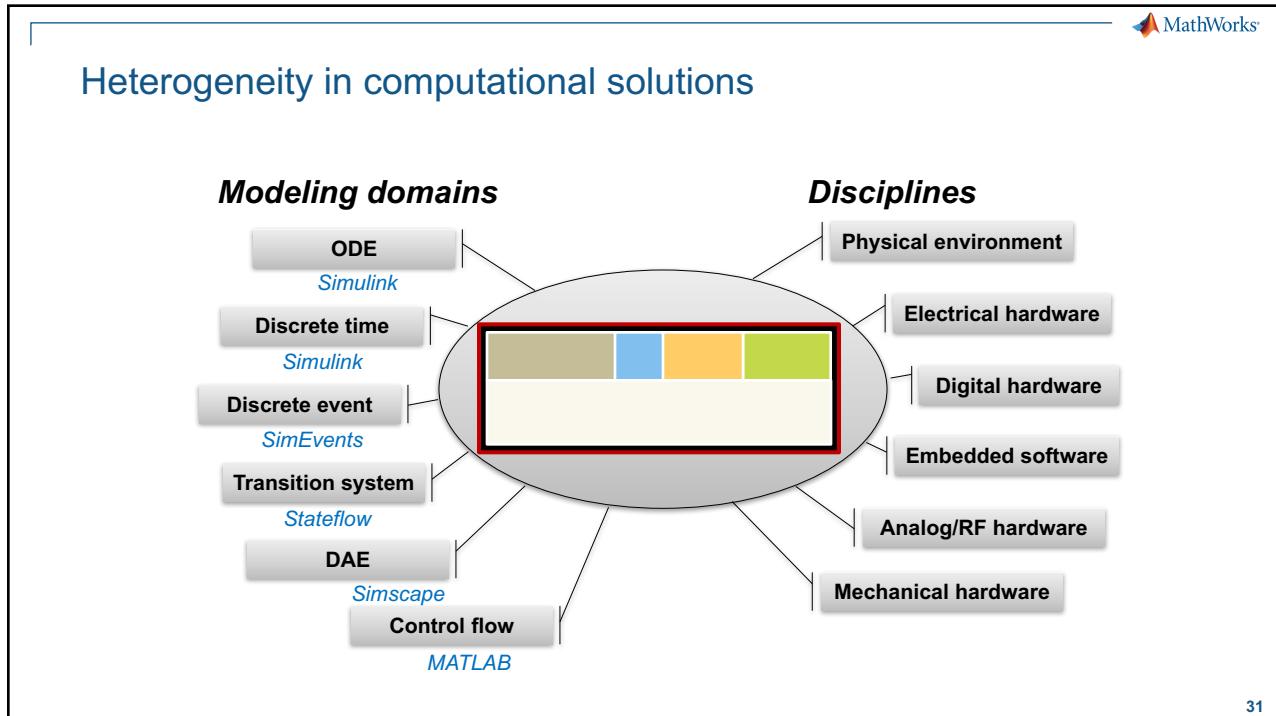
29

Design of heterogeneous systems

- Executable models
 - Quick feedback on design options
 - Automate design tasks
 - Automate synthesis tasks
 - ...
- Computational semantics
- Execution engine
 - Combines many formalisms



30



 MathWorks

Challenges

- Scientific and technological challenges
 - **Heterogeneity**: Multi-domain, multi-scale, multi-disciplinary nature
- Socio-technical challenges
 - **Trustworthiness**: safety, security, privacy, dependability
 - **Standardization and policy development**
 - Understanding **human interaction** with CPS
- **Education and workforce training challenges**
 - 21st century CPS education and workforce training

33

 MathWorks



The slide features a black and white photograph of a destroyed urban landscape with rubble and debris. Overlaid on the scene are several orange-colored 3D wireframe models of a person, a car, and a construction excavator. In the upper right corner, there is a thought bubble containing a computer monitor displaying a video conference between two people, labeled "Mission Command and Control Center". To the left, a person is shown holding a smartphone. The title "Smart Emergency Response Saves Lives" is centered at the top in red text.

Figure 3. Concise SERS vision slide.
<http://smartamerica.org/teams/smart-emergency-response-system-sers/>

34

MathWorks

Foundations for Innovation in Cyber-Physical Systems
WORKSHOP REPORT
January 2013
Prepared by ENERGETICS INCORPORATED Columbia, Maryland 21046
For the NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST National Institute of Standards and Technology

STEERING COMMITTEE FOR FOUNDATIONS FOR INNOVATION IN CYBER-PHYSICAL SYSTEMS
This report was prepared through the collaborative efforts of the individuals named below. It reflects their expert contributions as well as the many insights generated at the Foundations for Innovation in Cyber-Physical Systems Workshop held March 15–16, 2012 in Rosemont, Illinois.

Committee Co-chairs
James Sztipanovits, Vanderbilt University
Susan Ying, Boeing

Steering Committee Members
Isaac Cohen, United Technologies Corporation
David Corwin, Boeing
Jim Davis, UCLA and Smart Manufacturing Leadership Coalition
Himanshu Khurana, Honeywell Automation and Control Solutions
Pieter J. Mosterman, MathWorks
Venkatachalam Prasad, Ford
Lomy Storno, Medtronic, Inc.

This report was prepared as an account of work sponsored by the National Institute of Standards and Technology (NIST). The views and opinions expressed herein do not necessarily state or reflect those of NIST. Citation of trade names and/or commercial products is made in this document in order to illustrate a point or concept. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for this purpose.

* Workshop Report: Foundations for Innovation in Cyber-Physical Systems, January 2013. <http://comms.energetics.com/NIST-CPSWorkshop/download.html>

COMPUTATION for HUMANITY
Information Technology to Advance Society
Edited by JUSTYNA ZANDER PIETER J. MOSTERMAN
CRC CRC Press Taylor & Francis Group

<http://msdl.cs.mcgill.ca/people/mosterman/>

35

MathWorks

Challenges

- Scientific and technological challenges
 - **Heterogeneity**: Multi-domain, multi-scale, multi-disciplinary nature
- Socio-technical challenges
 - **Trustworthiness**: safety, security, privacy, dependability
 - **Standardization and policy** development
 - Understanding **human interaction** with CPS
- **Education and workforce training** challenges
 - Next-generation CPS education and workforce training

36

MathWorks

Contribution to education as an industry researcher

Carnegie Mellon



WPI

Foundations of Cyber-Physical Systems
CPS V&V Grand Prix student competition

Autonomous Vehicle Concentration
Summer School on Connected Autonomous Vehicles

PhD thesis committee

37

MathWorks



Jonathan Sprinkle
Litton Industries John M. Leonis Distinguished Associate Professor
Office: ECE 456N
Phone: 520.626.0737
Email: sprinkle@ece.arizona.edu
[Research/Lab Website](#)

A COLLEGE OF ENGINEERING
Electrical & Computer Engineering

Academia

Student Home | MATLAB Student | Tutorials | Examples | Student Competitions | Books | Hardware Support

CAT Vehicle Challenge

The CAT Vehicle CPS Challenge 2017 brings together 30 teams, comprised of over 80 students, to use Model-Based Design to develop a software component for controlling a real self-driving car—the University of Arizona's CAT Vehicle. The teams will create ROS software components prototyped using Simulink using real-world data from the CAT Vehicle to compete for tasks such as obstacle identification using fewest sensors possible, velocity computation for trajectory following, and generation of 3D simulation virtual world files in Gazebo from simulation trajectories and actual driving data. Top-performing teams will have an opportunity to see their validated software running on the CAT Vehicle in Tucson, AZ, over a period of 2-3 days.

Getting Started

See all the videos of the CAT Vehicle Simulator in action

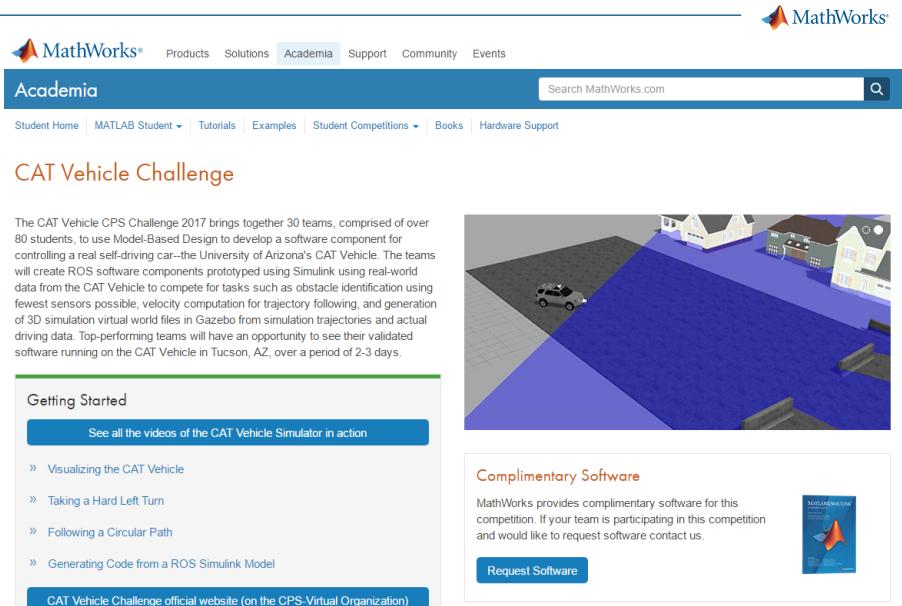
- » Visualizing the CAT Vehicle
- » Taking a Hard Left Turn
- » Following a Circular Path
- » Generating Code from a ROS Simulink Model

[CAT Vehicle Challenge official website \(on the CPS Virtual Organization\)](#)

Complimentary Software

MathWorks provides complimentary software for this competition. If your team is participating in this competition and would like to request software contact us.

[Request Software](#)



<https://www.mathworks.com/academia/student-competitions/catvehiclechallenge.html>

The Towers of Hanoi as a Cyber-Physical System Education Case Study

Pieter J. Mosterman
Design Automation Research
and Development
MathWorks
Natick, Massachusetts 01760-2098
pieter.mosterman@mathworks.com

Justyna Zander
Education Marketing
MathWorks
Natick, Massachusetts 01760-2098
justyna.zander@mathworks.com

Zhi Han
Design Automation Research
and Development
MathWorks
Natick, Massachusetts 01760-2098
zhi.han@mathworks.com

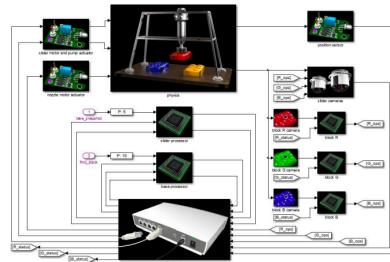


Fig. 2. Simulink® Model of the Distributed Towers of Hanoi

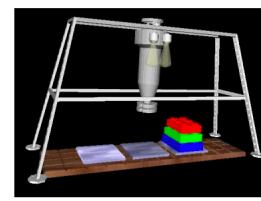


Fig. 3. The Synthesized Towers of Hanoi Scene

<https://www.mathworks.com/content/dam/mathworks/mathworks-dot-com/discovery/supporting-docs/towers-of-hanoi-as-cyber-physical-system.pdf> 39

Opportunities

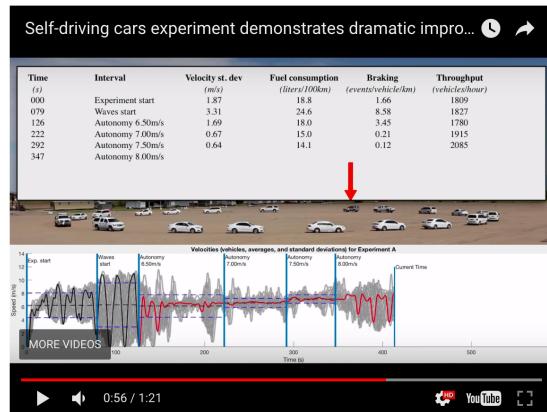
Small changes can already make a big impact!

Experiments show that a few self-driving cars can dramatically improve traffic flow



"Before we carried out these experiments, I did not know how straightforward it could be to positively affect the flow of traffic," Sprinkle said. "I assumed we would need sophisticated control techniques, but what we showed was that controllers which are staples of undergraduate control theory will do the trick."

<https://phys.org/news/2017-05-self-driving-cars-traffic.html>



<https://www.youtube.com/watch?v=2mBjYZTeaTc>

4

Opportunity for a transformative impact at a societal-scale!

42

