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

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

About me

Cummins — Research and Development, Application Engineering

Penn — MS, Research Staff

BOSCH — Research Intern

Carnegie Mellon — PhD

MathWorks

Advanced Research & Technology Office

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

2

Outline

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

3

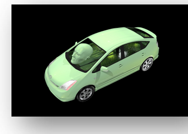
Tomorrow's systems are envisioned to be smart

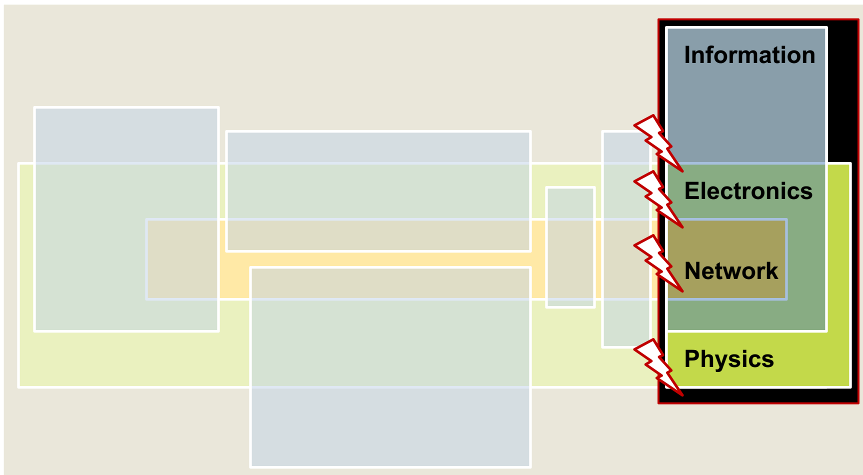
- Smart energy
- Smart mobility
- Smart health
- Smart manufacturing
- Smart cities

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

4

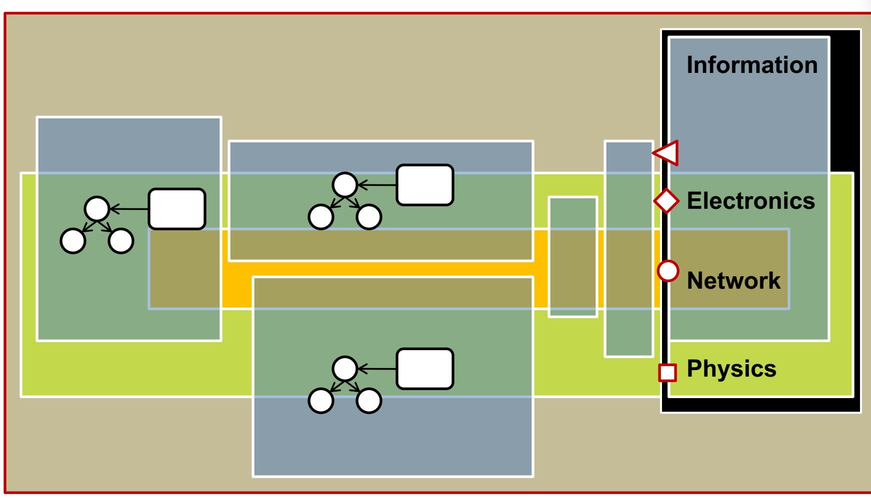
Networked embedded systems





5

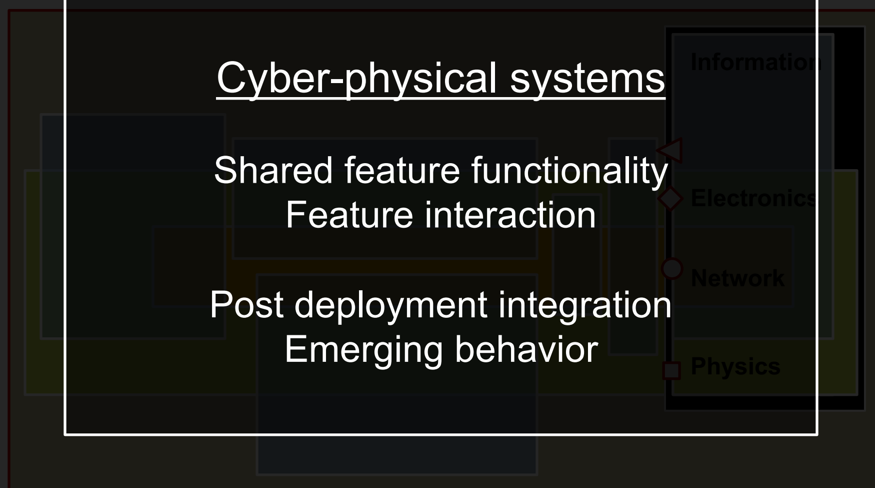
Cyber-physical systems



6

MathWorks

Cyber-physical systems



Cyber-physical systems

Shared feature functionality
Feature interaction

Post deployment integration
Emerging behavior

7

MathWorks

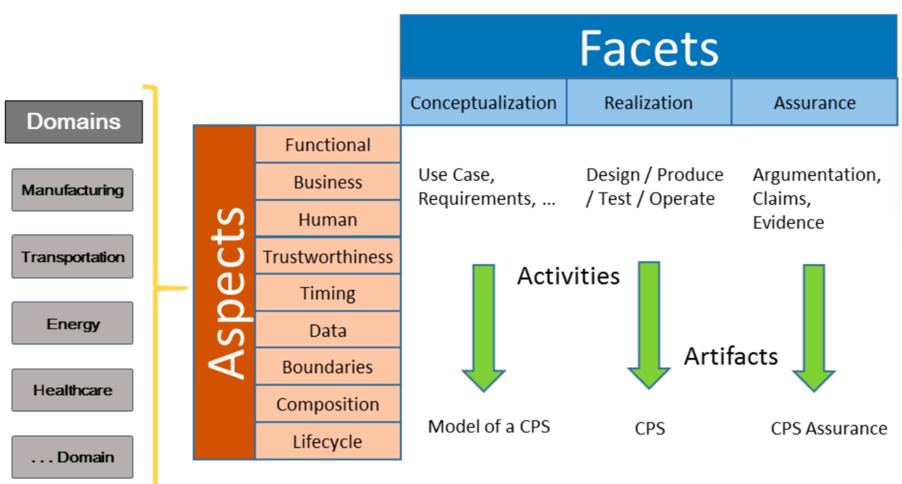
A feature characterization for smart systems

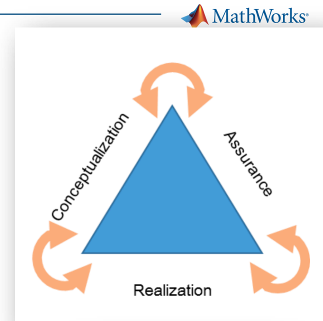
8

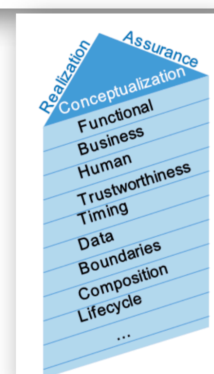
How do we characterize and develop ‘smartness’?

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

NIST CPS Framework – Facets







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

MathWorks

How do we characterize and develop smarts?

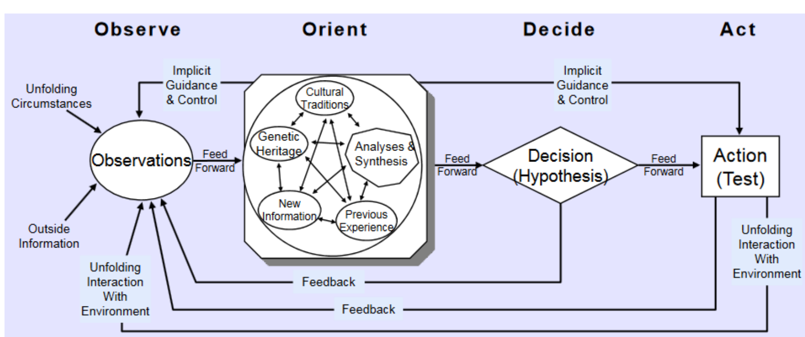
- Smart energy
- Smart mobility
- Smart health
- Smart manufacturing
- Smart cities

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

11

MathWorks

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

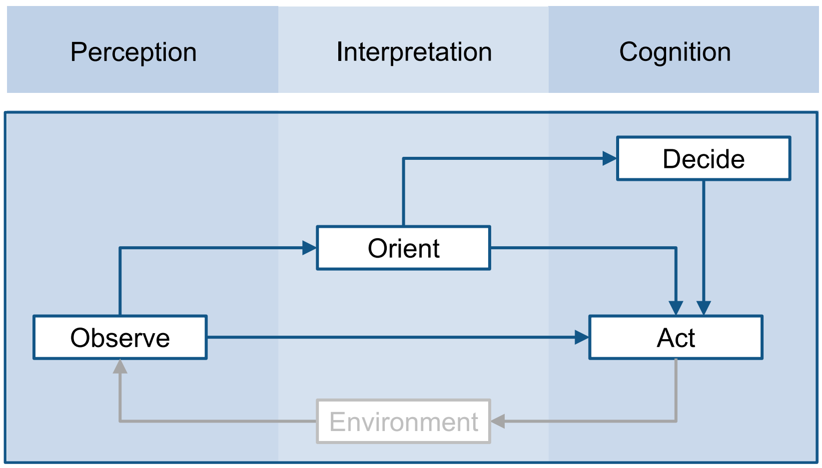


https://en.wikipedia.org/wiki/John_Boyd_(military_strategist)#The_OODA_Loop

12

MathWorks

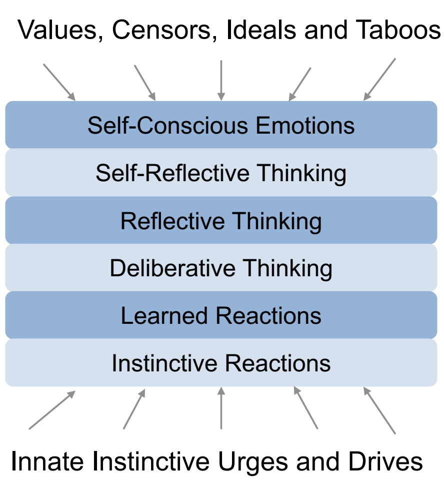
OODA loop and the stages of cognition



13

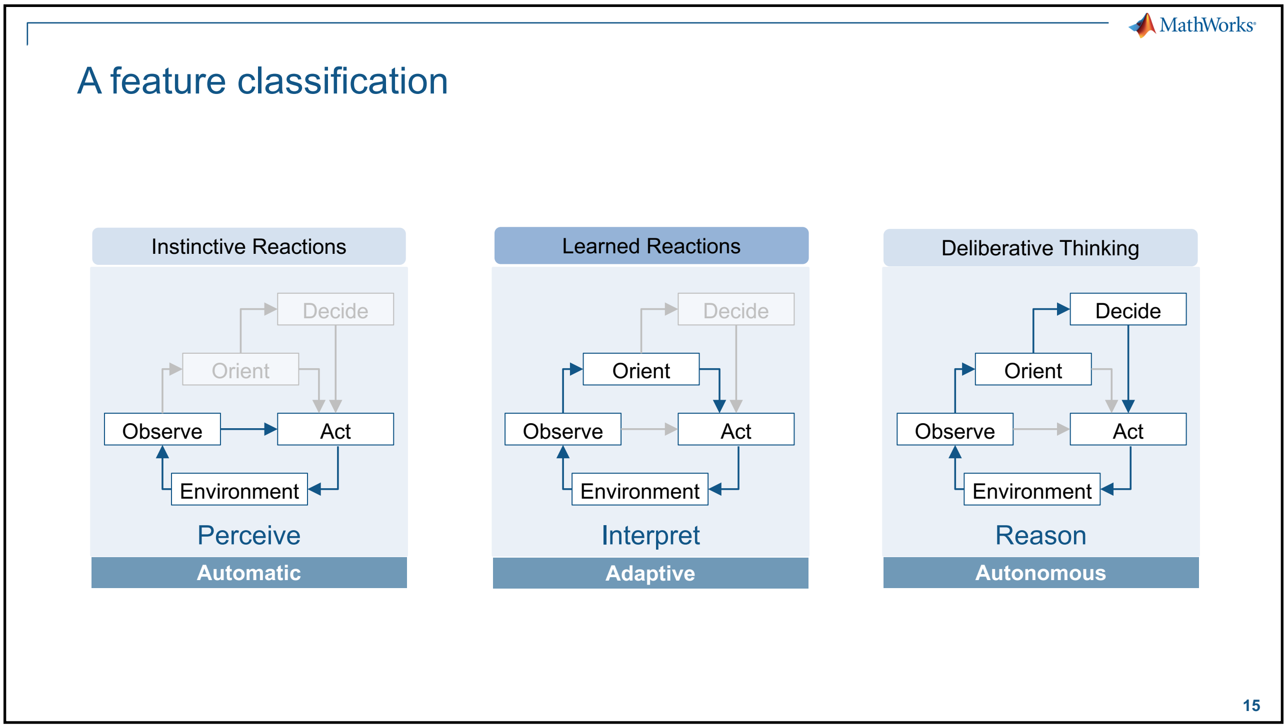
MathWorks

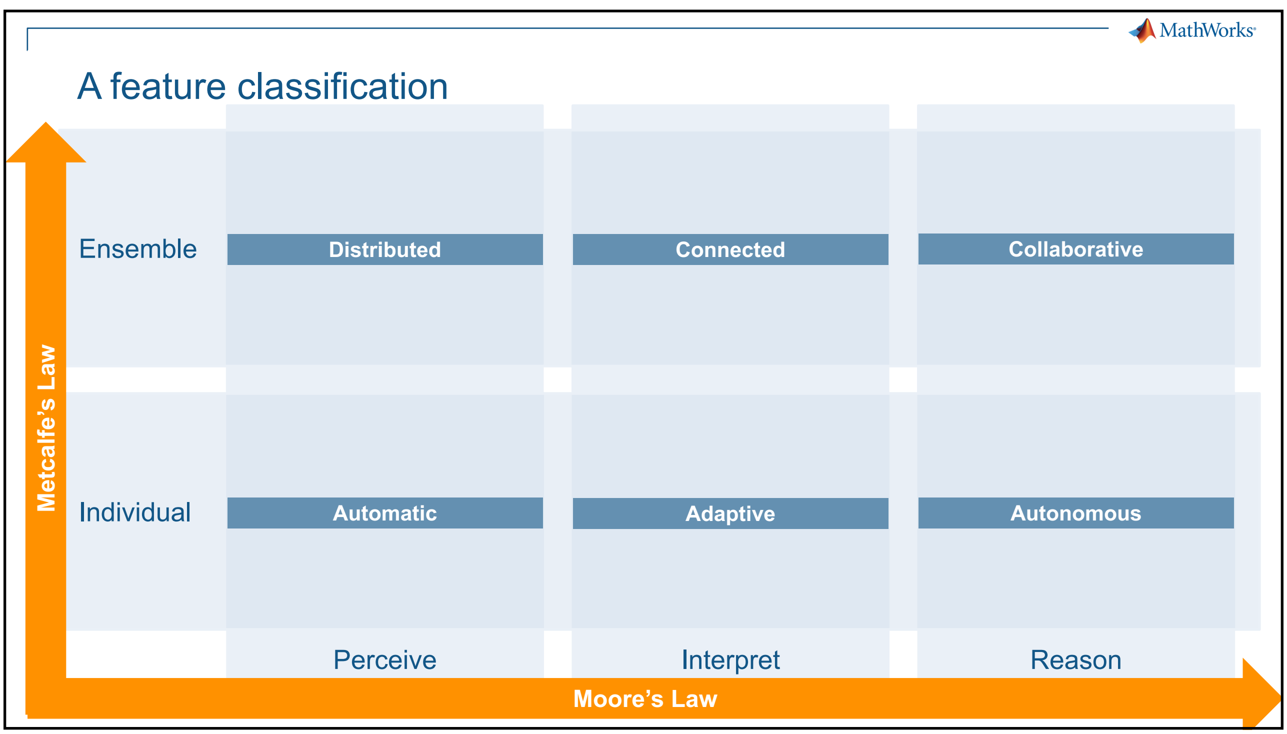
OODA loop and Marvin Minsky's *Levels of Mental Activities*



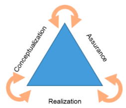
Redrawn from https://web.media.mit.edu/~minsky/eb5.html

14


MathWorks
A feature classification
Instinctive Reactions
Decide
Orient
Observe
Act
Environment
Perceive
Automatic
Learned Reactions
Decide
Orient
Observe
Act
Environment
Interpret
Adaptive
Deliberative Thinking
Decide
Orient
Observe
Act
Environment
Reason
Autonomous
15


MathWorks
A feature classification
Metcalfe's Law
Ensemble
Distributed
Connected
Collaborative
Individual
Automatic
Adaptive
Autonomous
Perceive
Interpret
Reason
Moore's Law

MathWorks

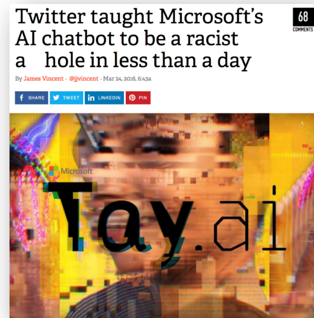


Adaptive

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

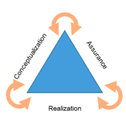
https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

"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

MathWorks



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?

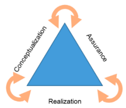
Assure
- How to test a self-changing artifact?
  - If regimes are not pre enumerated?
- Ensure successful and correct online calibration?


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

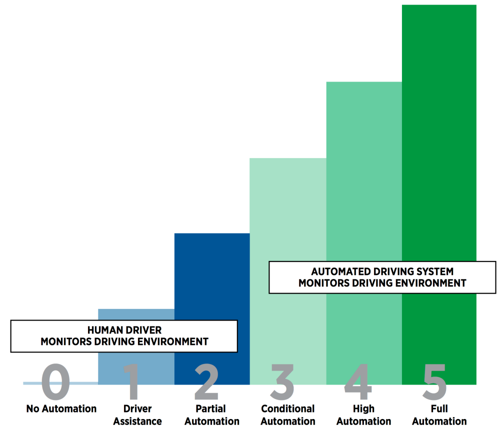


Autonomous

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?

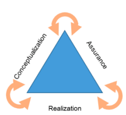
Assure
- Turing test for cars?
- Ensure the reasoning is always safe?
- Degraded safety (there is no perfect safety)?



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 19

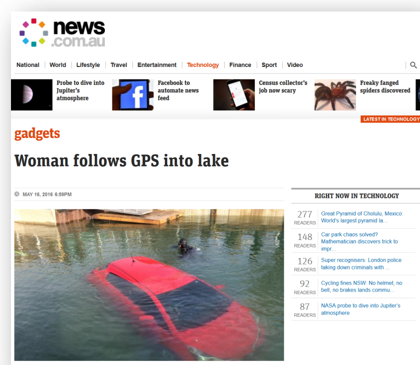


Connected

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

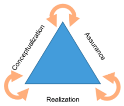
Realize
- Safely operate in the face of communication challenges
  - Degradation, loss
  - Corruption
- Timeliness and responsiveness guarantees?
  - Service discovery time out, DoS

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 20

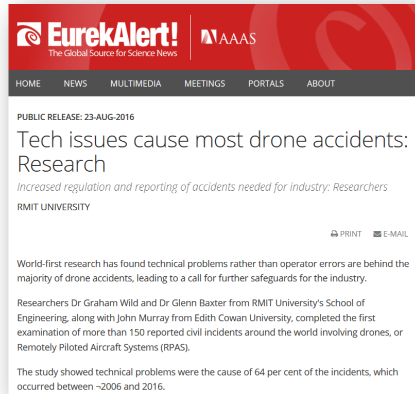


Connected

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?


EurekAlert! The Global Source for Science News AAAS

HOME NEWS MULTIMEDIA MEETINGS PORTALS ABOUT

PUBLIC RELEASE: 23-AUG-2016

Tech issues cause most drone accidents: Research

Increased regulation and reporting of accidents needed for industry: Researchers

RMIT UNIVERSITY

PRINT E-MAIL

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.

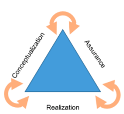
Researchers Dr Graham Wild and Dr Glenn Baxter from RMIT University's School of Engineering, along with John Murray from Edith Cowan University, completed the first examination of more than 150 reported civil incidents around the world involving drones, or Remotely Piloted Aircraft Systems (RPAS).

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/ru-tic082216.php

21

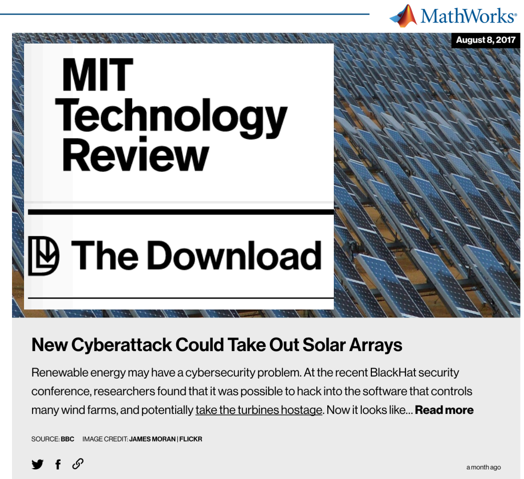


Connected

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?


August 8, 2017

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**

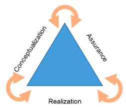
SOURCE: BBC IMAGE CREDIT: JAMES MORAN | FLICKR

a month ago

"… 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

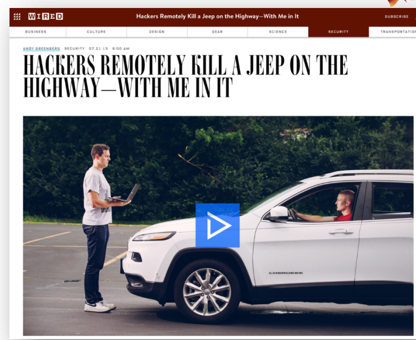


Connected

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?

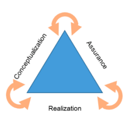


"Uconnect's cellular connection also lets anyone who knows the car's IP address gain access from anywhere in the country."

"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/

23

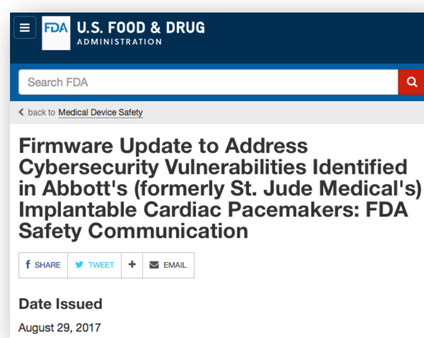


Connected

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?

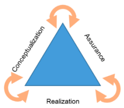


"these vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment.

https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

24

MathWorks



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?


BBC NEWS WORLD EDITION
You are in: Europe
Tuesday, 2 July, 2002, 14:07 GMT 15:07 UK
Crash planes dived to disaster
A flight recorder from the Tupolev has been recovered
A passenger jet and a cargo plane which collided in mid-air in southern Germany were both diving to avoid each other, it has emerged.

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

MathWorks

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 New York Times
TECHNOLOGY
Google's Driverless Cars Run Into Problem: Cars With Drivers

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

MathWorks

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

MathWorks

Research Questions

Carnegie Mellon University
Research Showcase @ CMU

Dissertations | Theses and Dissertations

5-2013

Multi-Model Heterogeneous Verification of Cyber-Physical Systems

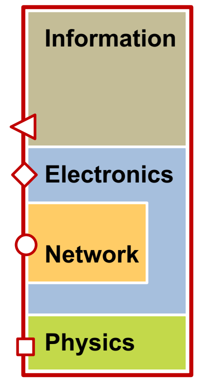
Akshay H. Rajhans
Carnegie Mellon University

28

MathWorks

Design of heterogeneous systems

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

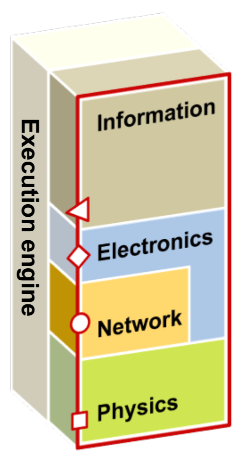


29

MathWorks

Design of heterogeneous systems

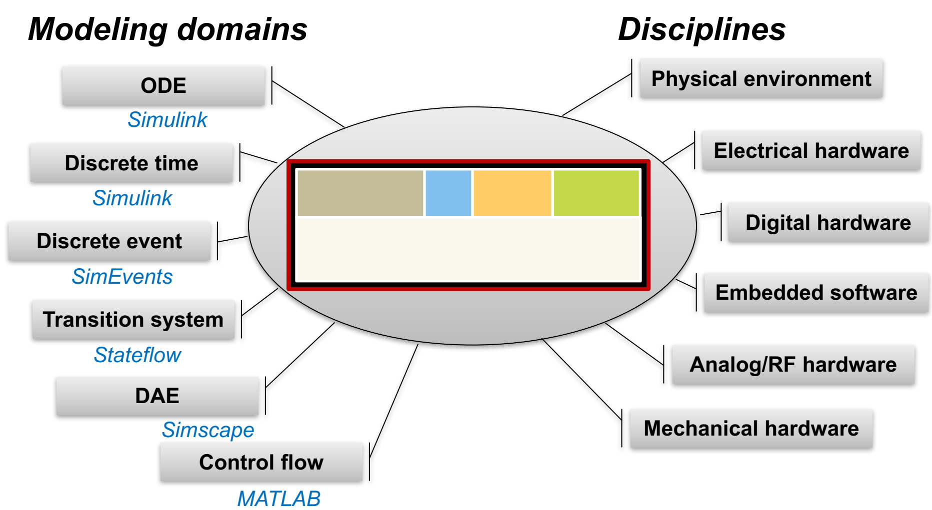
- Executable models
  - Quick feedback on design options
  - Automate design tasks
  - Automate synthesis tasks
  - …
- Computational semantics
- Execution engine
  - Combines many formalisms



30

MathWorks

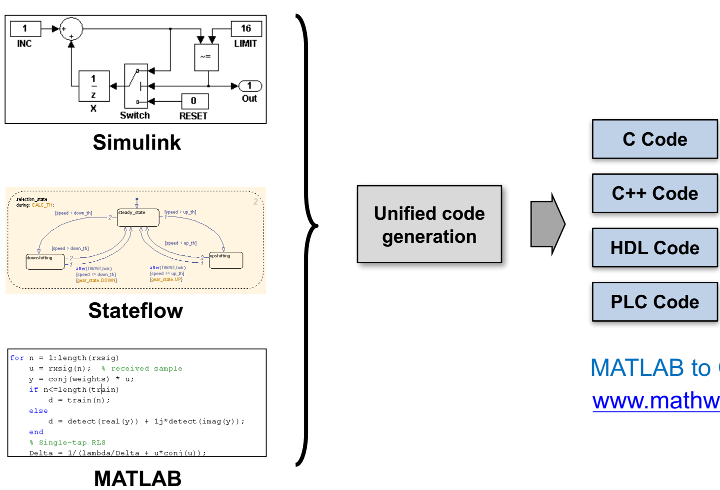
Heterogeneity in computational solutions



31

MathWorks

Code Generation: Multi-Language Support



MATLAB to CUDA compiler: beta program
www.mathworks.com/matlab-cuda-beta

32

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

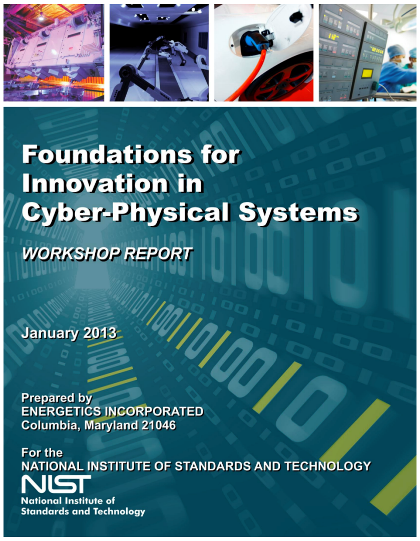
33

Figure 3. Concise SERS vision slide.

http://smartamerica.org/teams/smart-emergency-response-system-sers/

34

MathWorks



STEERING COMMITTEE FOR FOUNDATIONS FOR INNOVATION IN CYBER-PHYSICAL SYSTEMS

This report was prepared through the collaborative efforts of the individuals noted 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 13-14, 2012 in Rosemont, Illinois.[1]

Committee Co-chairs

Janos Sztipanovits, Vanderbilt University

Susan Ying, Boeing

Steering Committee Members

Isaac Cohen, United Technologies Corporations

David Corman, Boeing

Jim Davis, UCLA and Smart Manufacturing Leadership Coalition

Himanshu Khurana, Honeywell Automation and Control Solutions

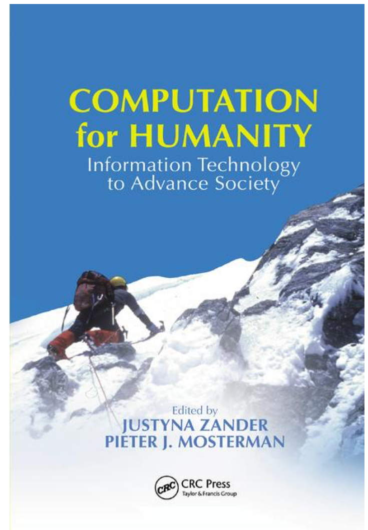
Pieter J. Mosterman, MathWorks

Venkatesh Prasad, Ford

Lonny Stormo, Medtronic, Inc.

This report was prepared as an account of work cosponsored by the National Institute of Standards and Technology (NIST). The views and opinions expressed herein do not necessarily state or reflect those of NIST. Certain commercial entities, equipment, or materials may be identified 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 the purpose.

[1] Workshop Report: Foundations for Innovation in Cyber-Physical Systems, January 2013. http://events.energetics.com/NIST-CPSWorkshop/downloads.html



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

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

WPI

Autonomous Vehicle Concentration

Summer School on Connected Autonomous Vehicles

Rensselaer

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

College of Engineering
Electrical & Computer Engineering

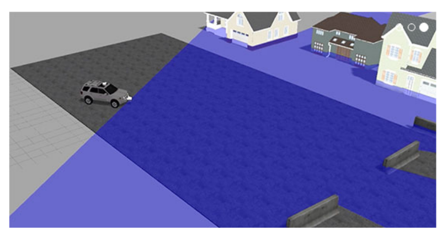
MathWorks Products Solutions Academia Support Community Events

Academia — Search MathWorks.com

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

38

MathWorks

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

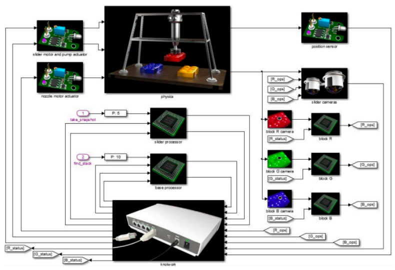


Fig. 2. Simulink® Model of the Distributed Towers of Hanoi

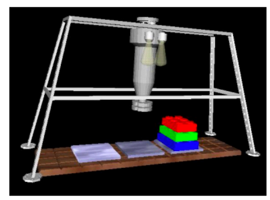


Fig. 3. The Synthesized Towers of Hanoi Scene

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

MathWorks

Opportunities

40

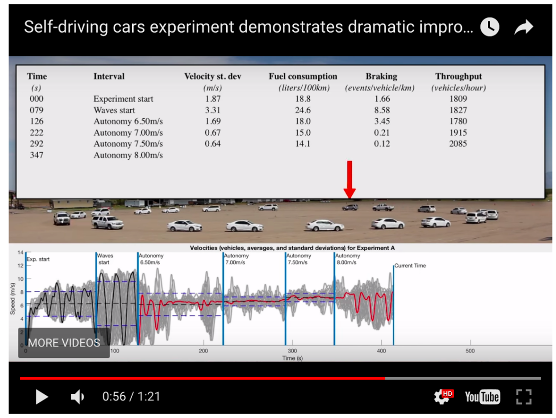
MathWorks

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



Time (s)	Interval	Velocity st. dev (m/s)	Fuel consumption (liters/100km)	Braking (events/vehicle/km)	Throughput (vehicles/hour)
000	Experiment start	1.87	18.8	1.66	1809
079	Waves start	3.31	24.6	8.58	1827
126	Autonomy 6.50m/s	1.69	18.0	3.45	1780
222	Autonomy 7.00m/s	0.67	15.0	0.21	1915
292	Autonomy 7.50m/s	0.64	14.1	0.12	2085
347	Autonomy 8.00m/s				

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

41

MathWorks

Opportunity for a transformative impact at a societal-scale!

42

MathWorks®

Accelerating the pace of engineering and science