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

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

About me

Research and Development
Application Engineering

MS
Research Staff

Research Intern

PhD

Advanced Research & Technology Office

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

Outline

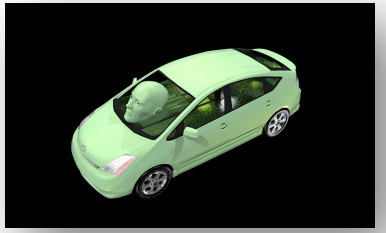
- What's unique about cyber-physical systems (CPS)
- A CPS feature classification
- Challenges
- Opportunities

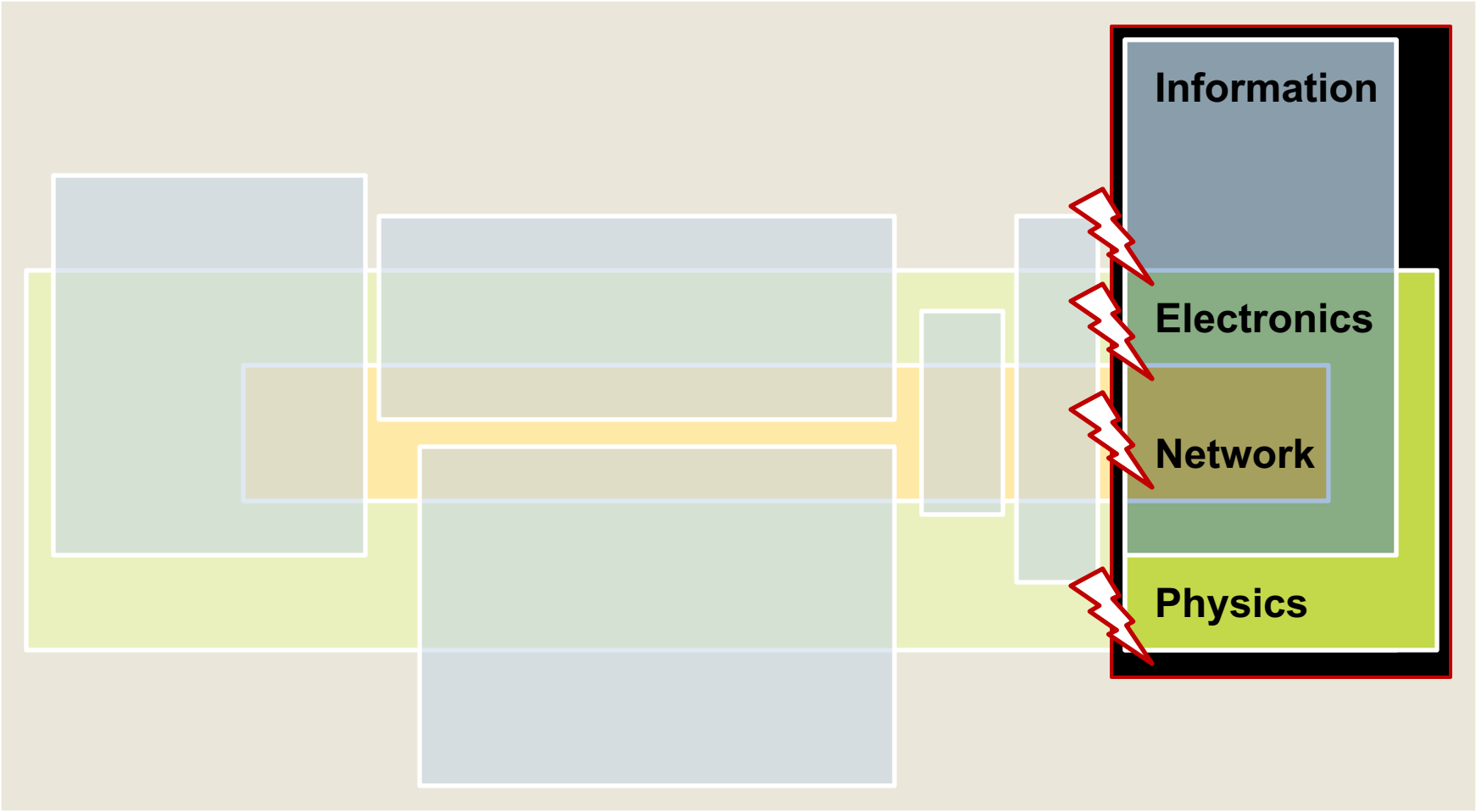
Tomorrow's systems are envisioned to be smart

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

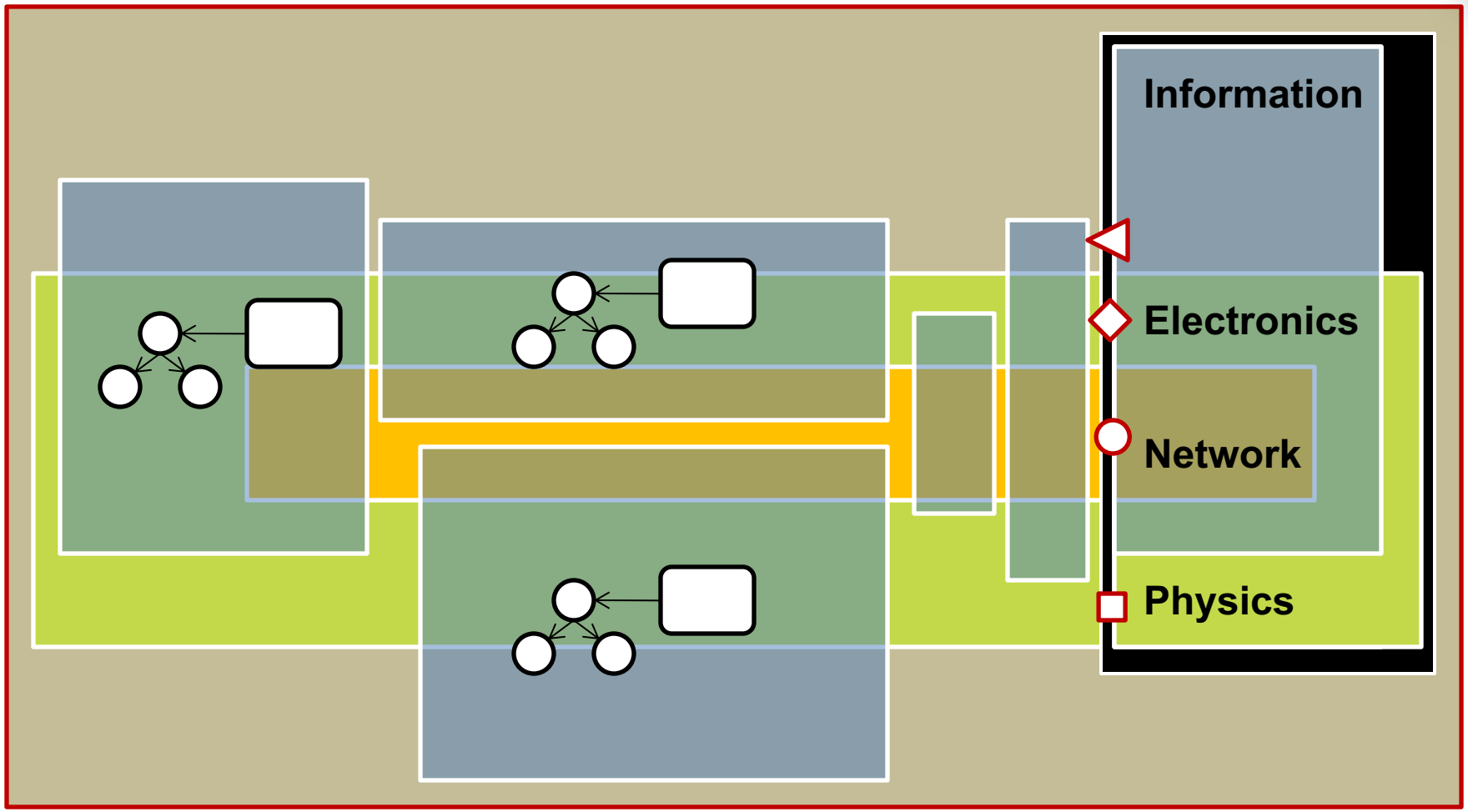
Q: How do we define, design, and develop the smarts?

Networked embedded systems

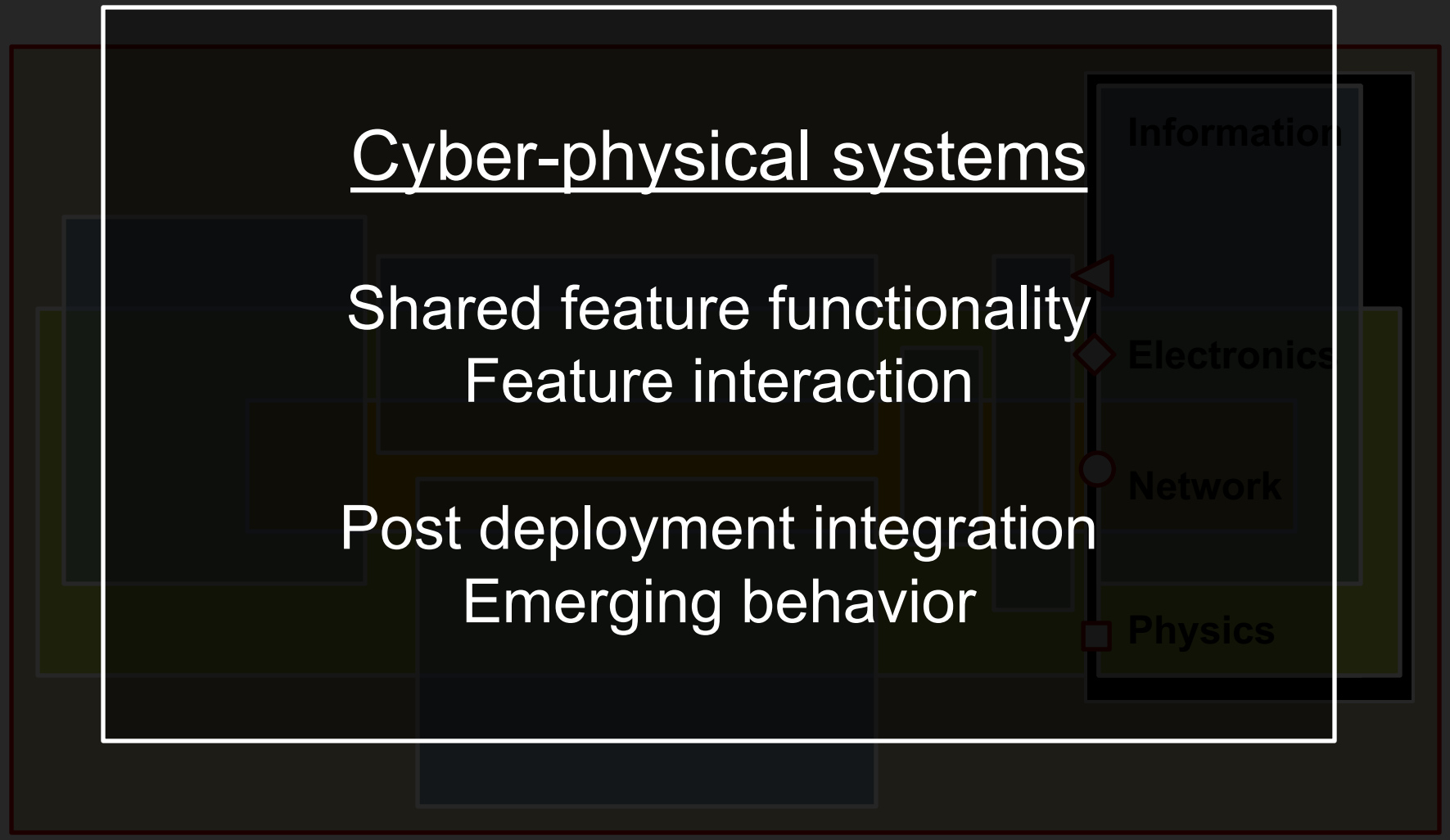




Cyber-physical systems



Cyber-physical systems

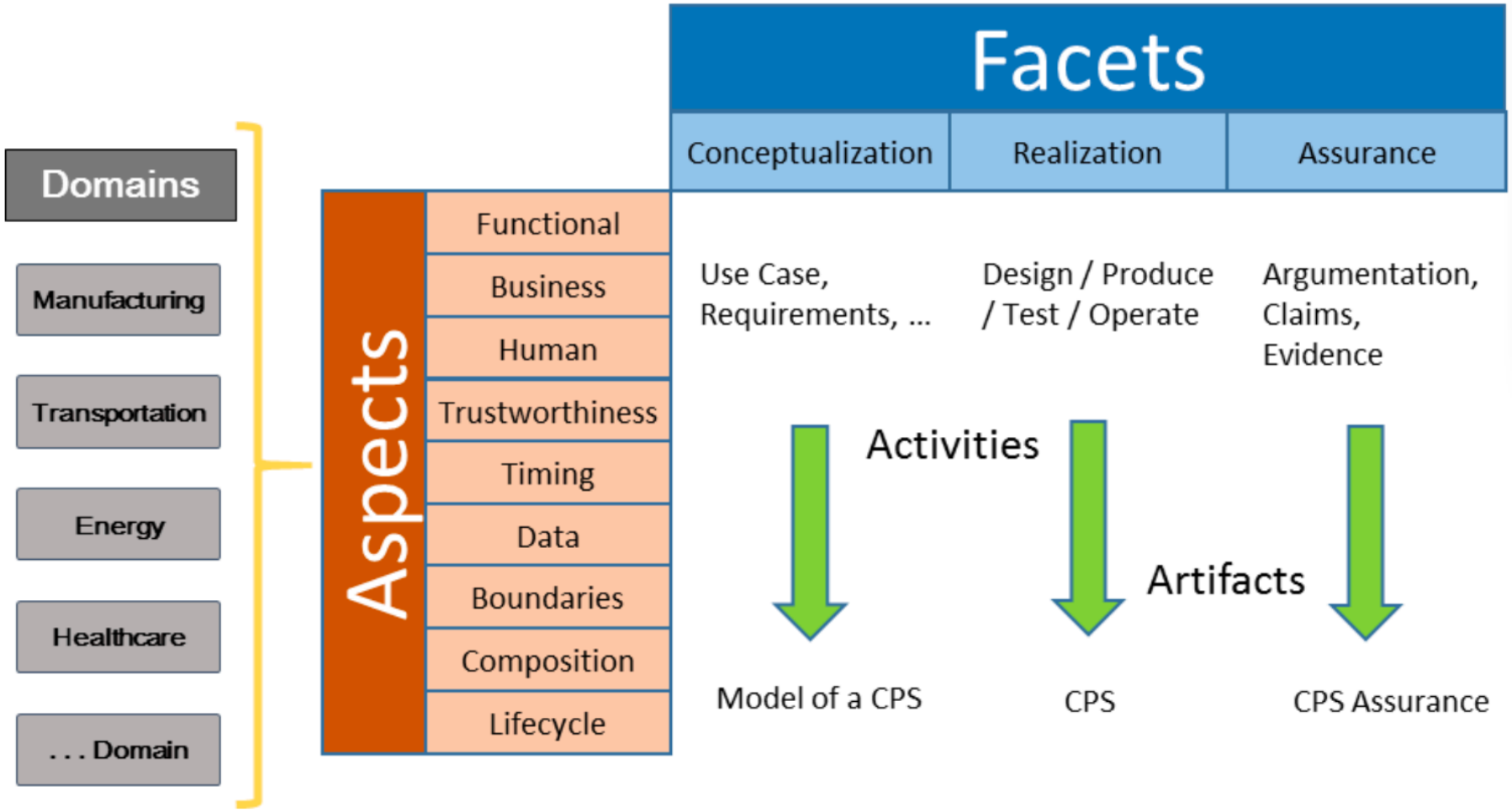


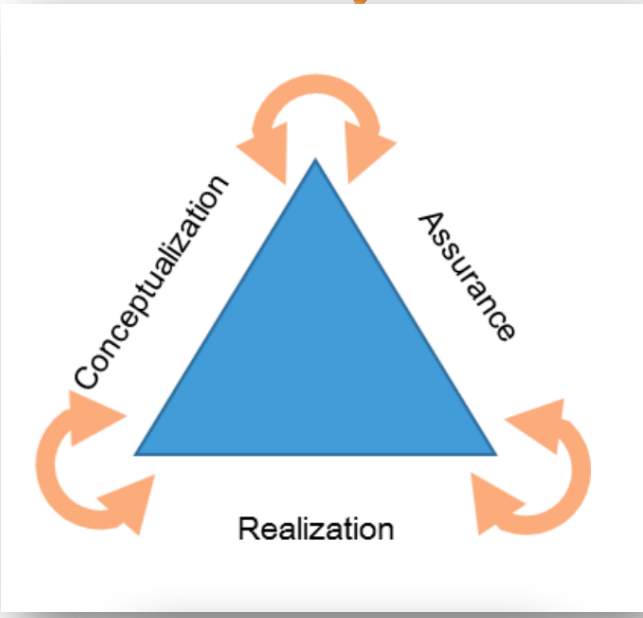
A feature characterization for smart systems

How do we characterize and develop ‘smartness’?

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

NIST CPS Framework – Facets





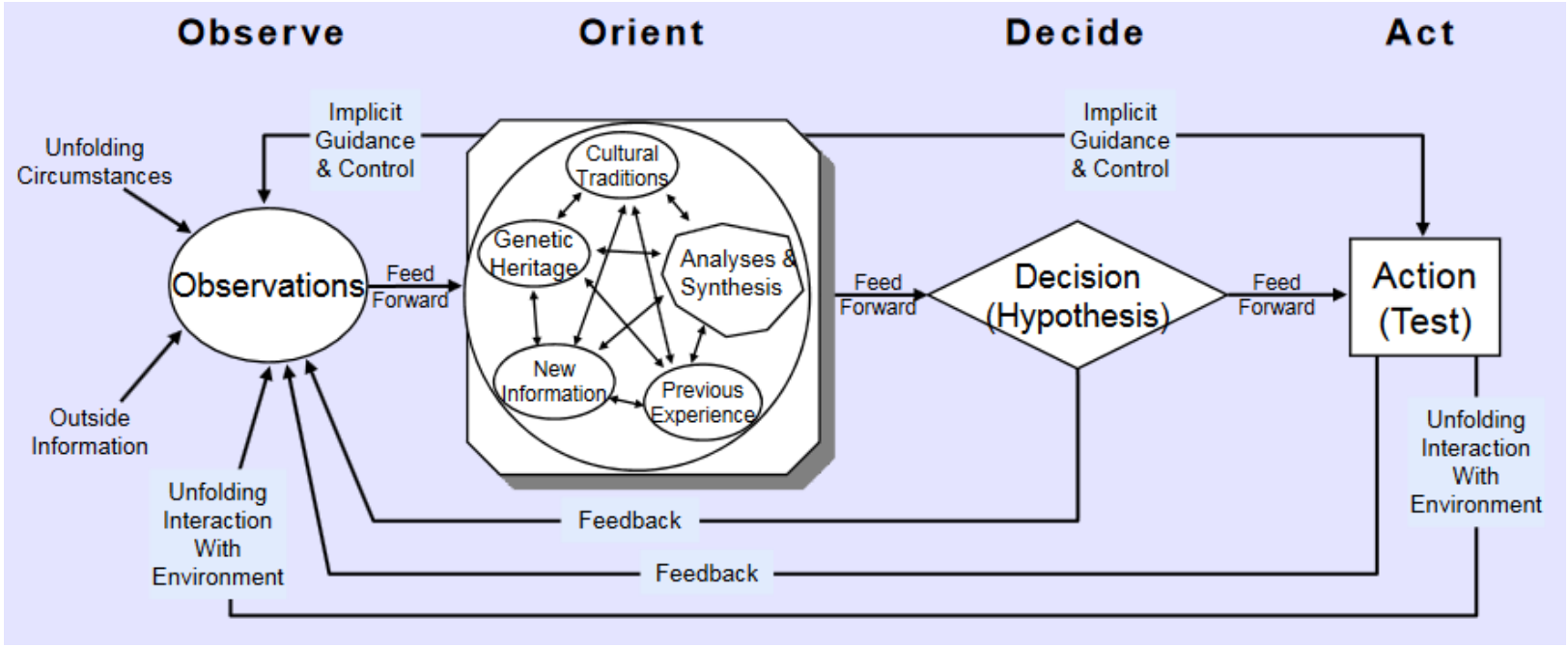
https://pages.nist.gov/cpspwg/

How do we characterize and develop smarts?

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

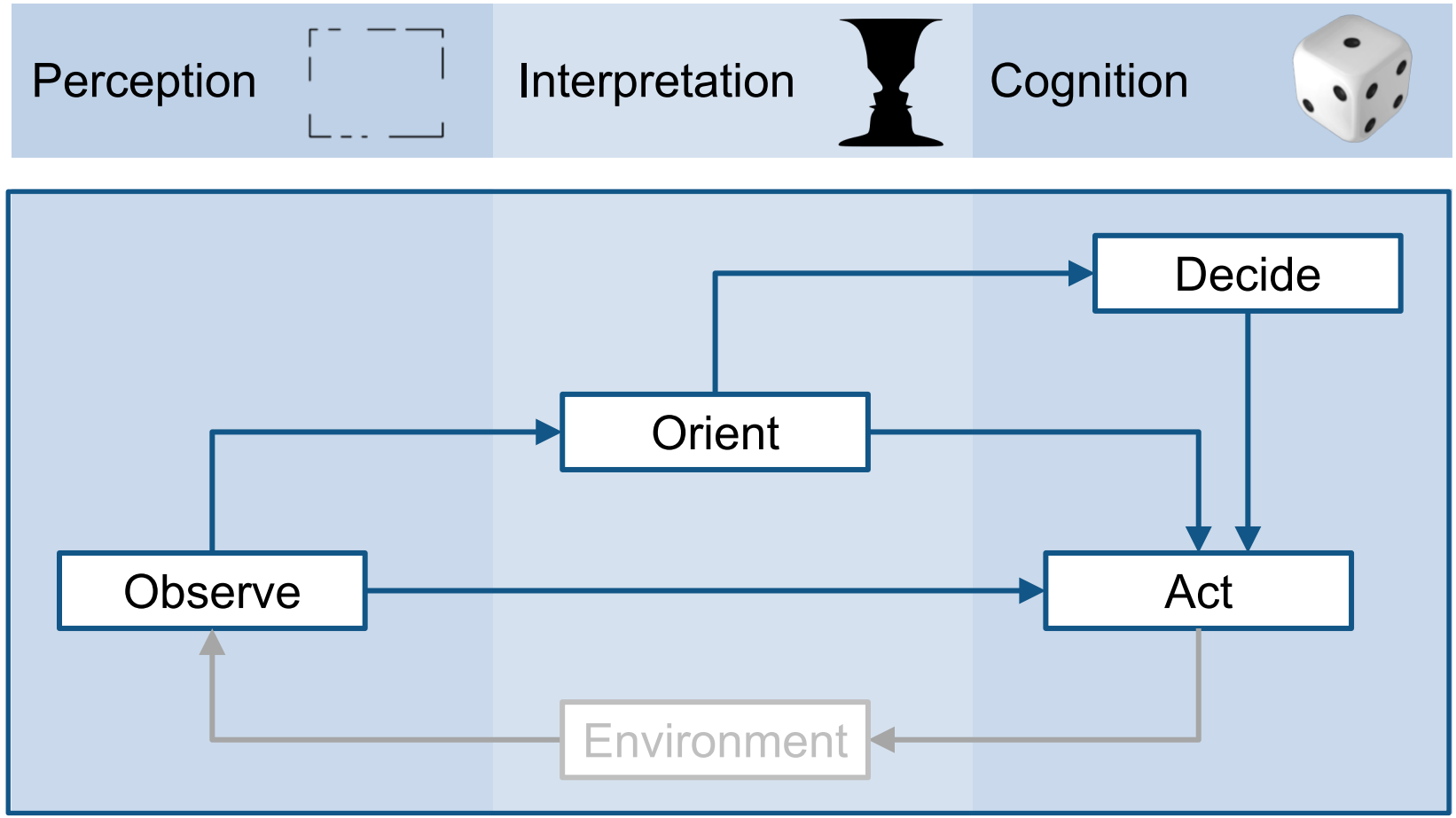
Q: How do we define, design, and develop smarts?

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

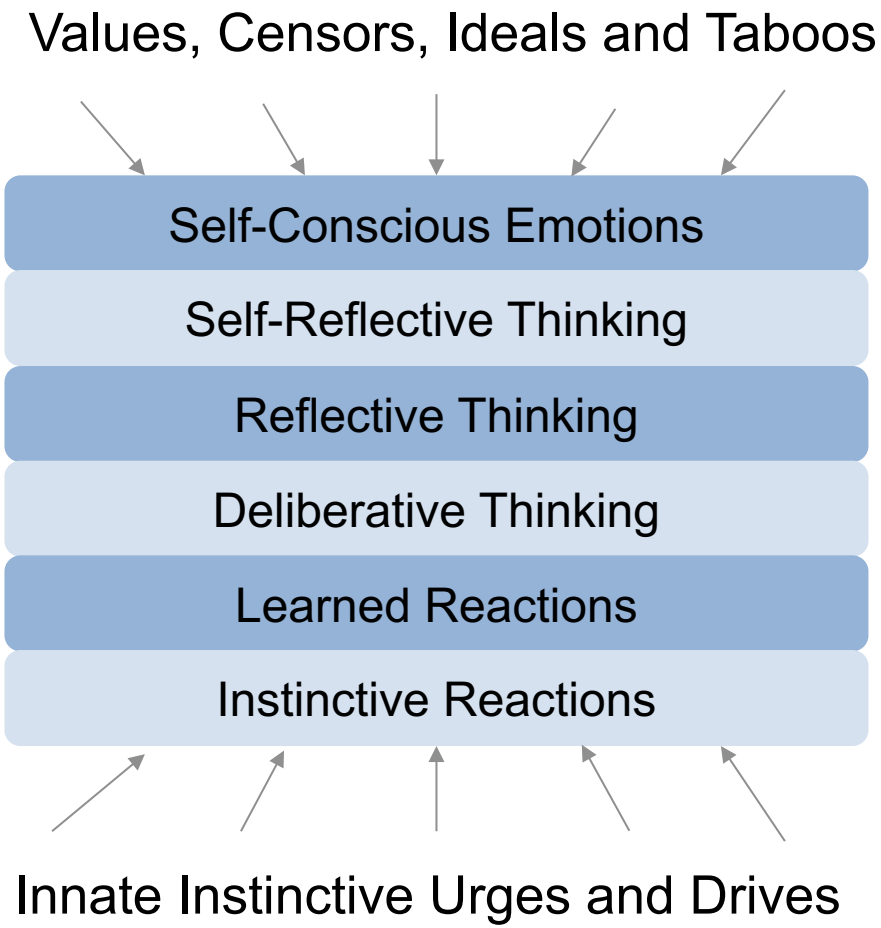


https://en.wikipedia.org/wiki/John_Boyd_(military_strategist)#The_OODA_Loop

OODA loop and the stages of cognition

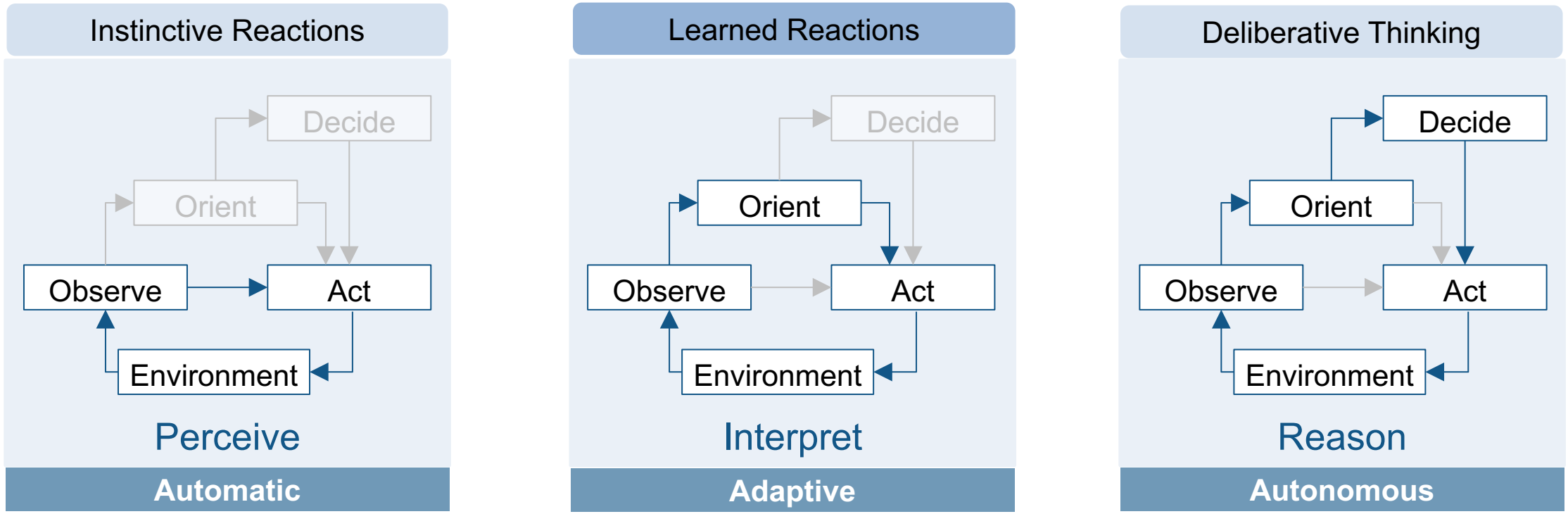


OODA loop and Marvin Minsky's *Levels of Mental Activities*

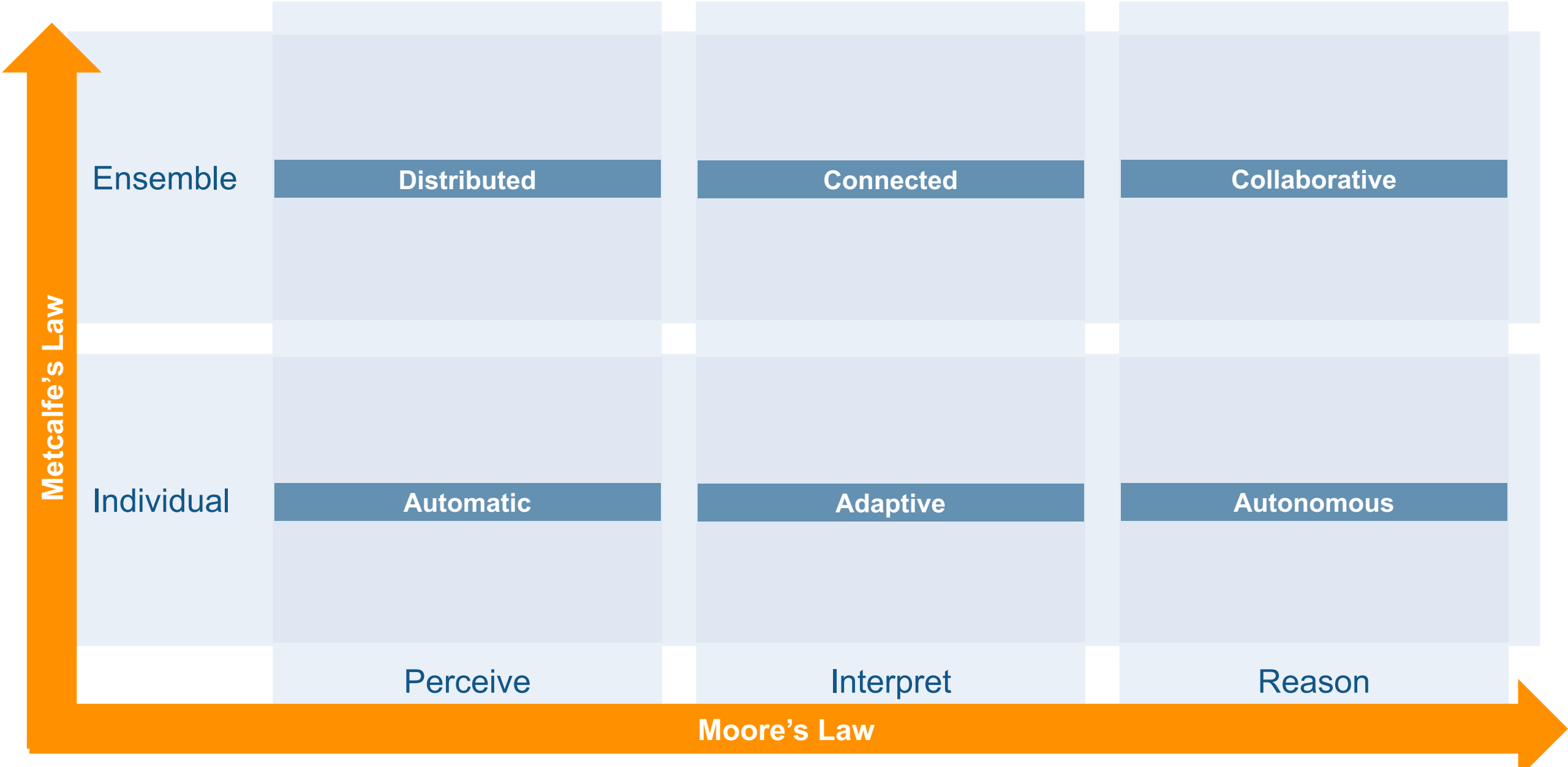


Redrawn from https://web.media.mit.edu/~minsky/eb5.html

A feature classification



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?

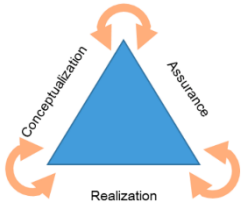
Assure
- How to test a self-changing artifact?
  - If regimes are not pre enumerated?
- Ensure successful and correct online calibration?

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

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’ ”

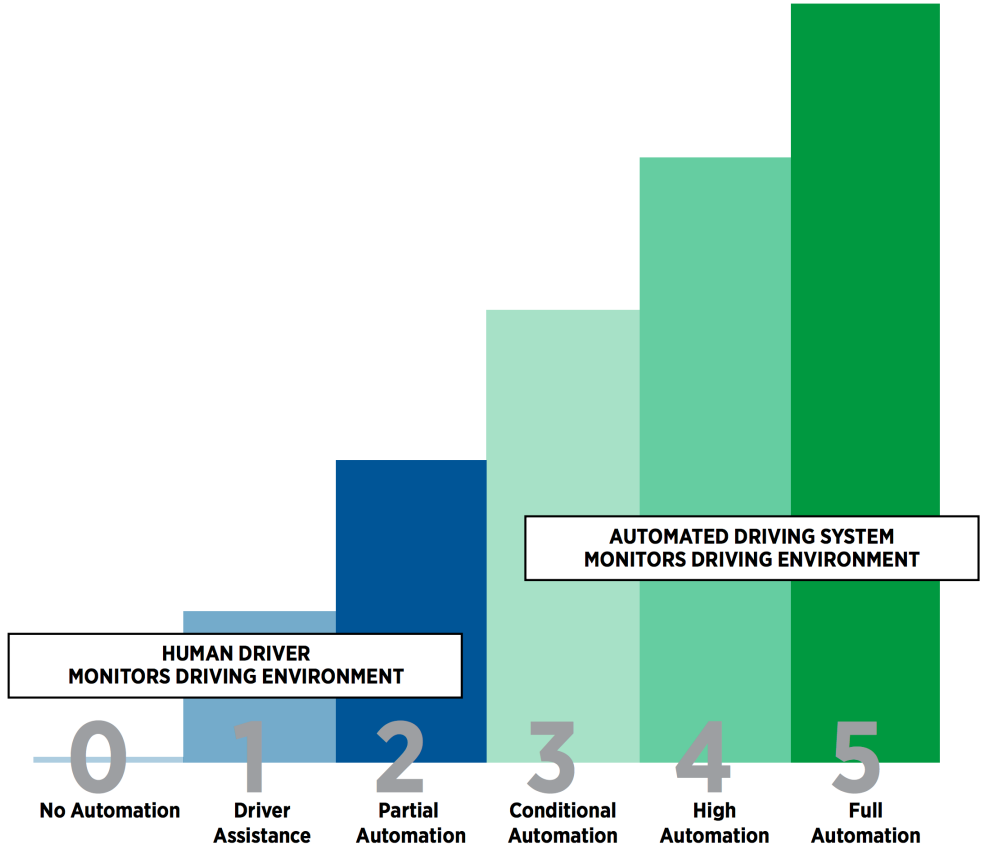
https://cacm.acm.org/news/217198-father-of-the-internet-ai-stands-for-artificial-idiot/fulltext

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

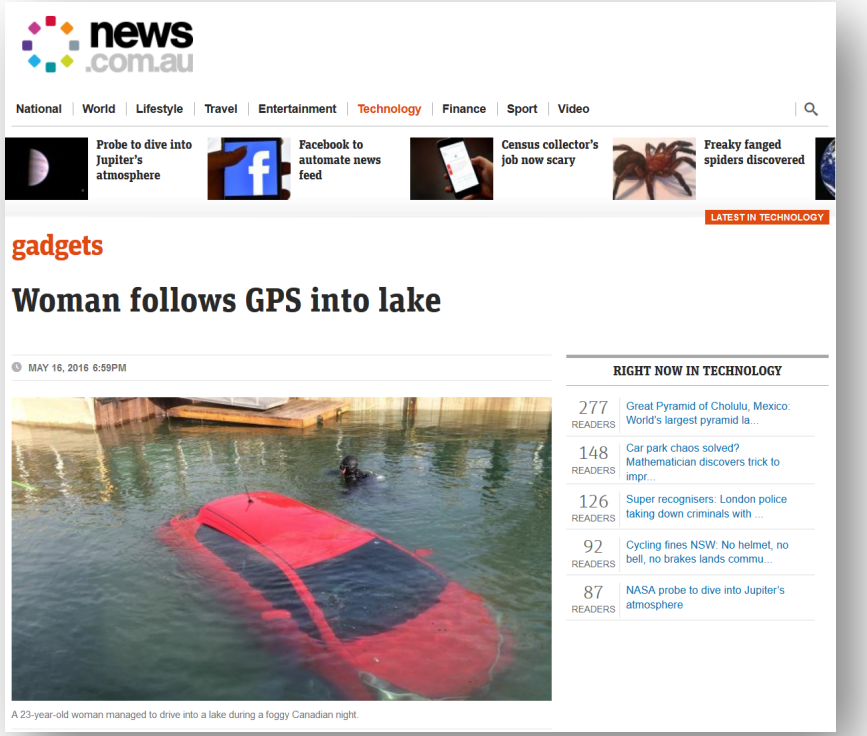
- How to interpret data safely
  - Which data to corroborate information?

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

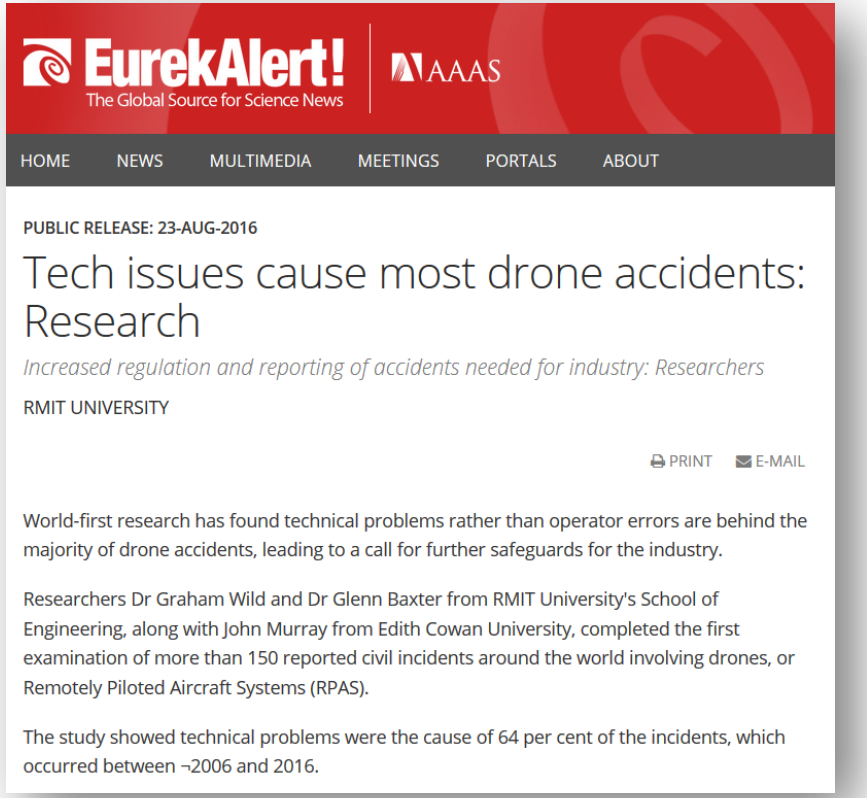
- How to interpret data safely
  - Which data to corroborate information?

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?



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.

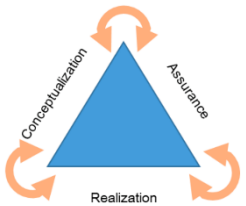
Researchers Dr Graham Wild and Dr Glenn Baxter from RMIT University's School of Engineering, along with John Murray from Edith Cowan University, completed the first examination of more than 150 reported civil incidents around the world involving drones, or Remotely Piloted Aircraft Systems (RPAS).

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

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?

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."

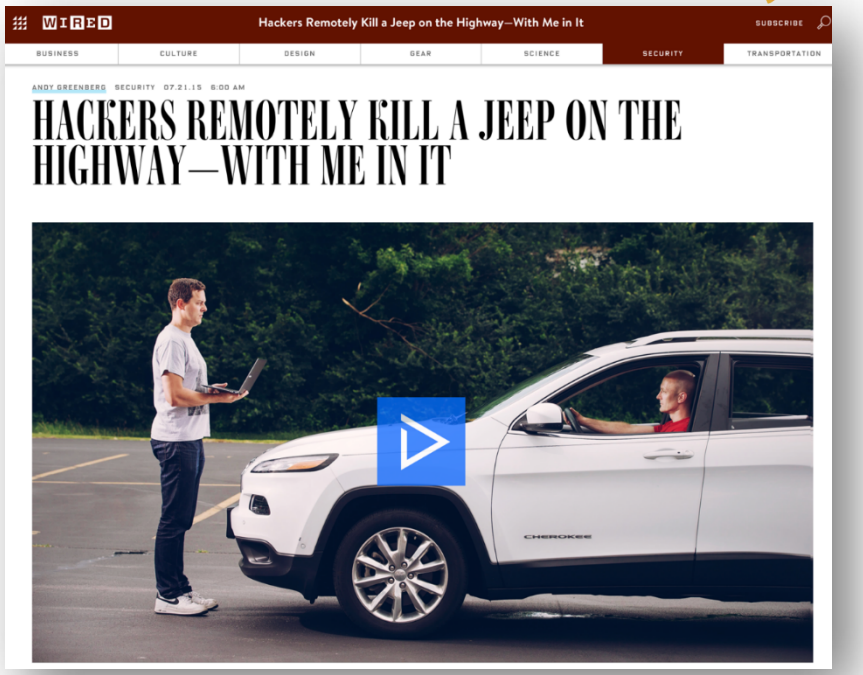
https://www.technologyreview.com/the-download/608588/new-cyberattack-could-take-out-solar-arrays/

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?

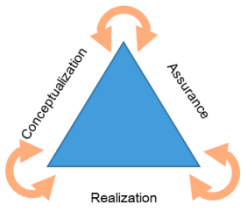


"Uconnect's cellular connection also lets anyone who knows the car's IP address gain access from anywhere in the country."

"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/

Connected



Conceptualize

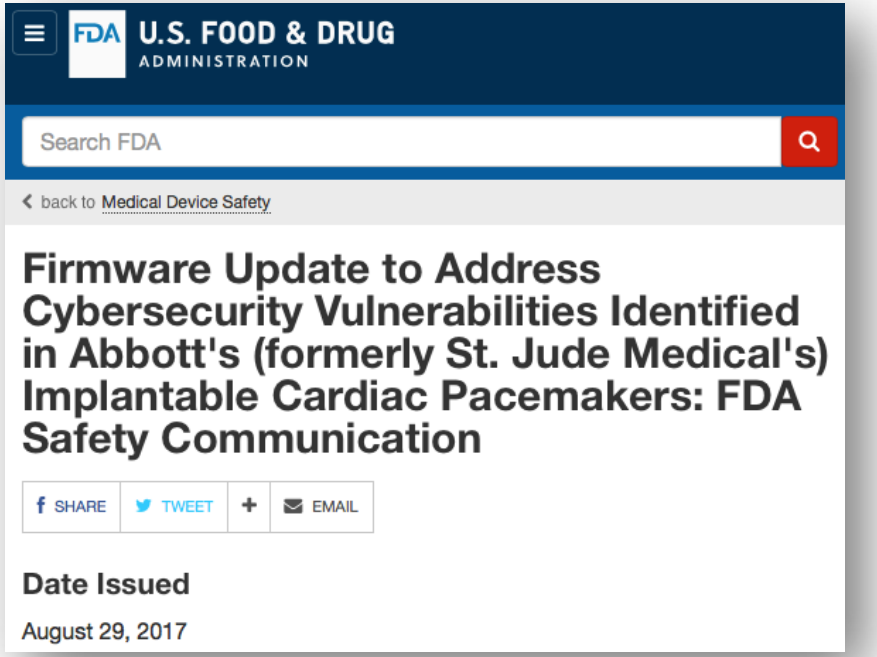
- How to interpret data safely
  - Which data to corroborate information?

Realize

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

Assure

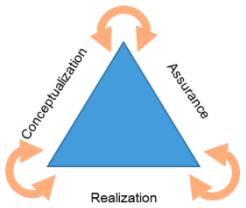
- Is closed loop verification possible?
- How do you obtain failure probabilities?



"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

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

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?

SECTIONS HOME SEARCH The New York Times LOG IN

BOYDTON JOURNAL
Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns

TECHNOLOGY

FEATURE
Inside Facebook's (Totally Insane, Unintentionally Gigantic, Hyperpartisan)...

Cycling Matches the Pace and Pitches of Tech

Adopted Koreans, Stymied in Search of Birth Parents, Find Hope in a Cotton Swab

TECHNOLOGY

Google's Driverless Cars Run Into Problem: Cars With Drivers

By MATT RICHTEL and CONOR DOUGHERTY SEPT. 1, 2015

855

A Google self-driving car in Mountain View, Calif. Google cars regularly take the most cautious approach, but that can put them out of step with the other vehicles on the road.
Gordon De Los Santos/Google

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

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

Research Questions

Carnegie Mellon University
Research Showcase @ CMU

Dissertations | Theses and Dissertations

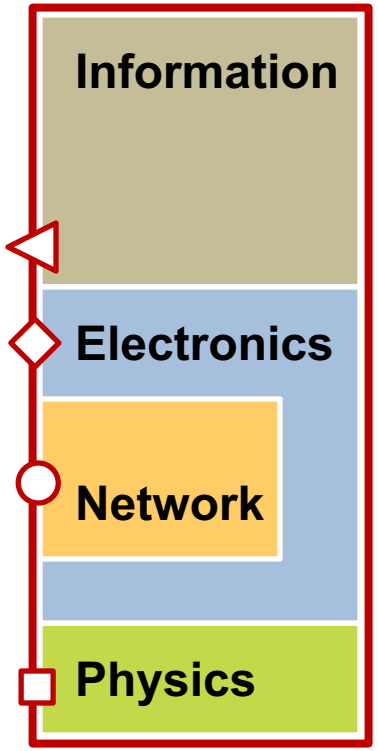
5-2013

Multi-Model Heterogeneous Verification of Cyber-Physical Systems

Akshay H. Rajhans
Carnegie Mellon University

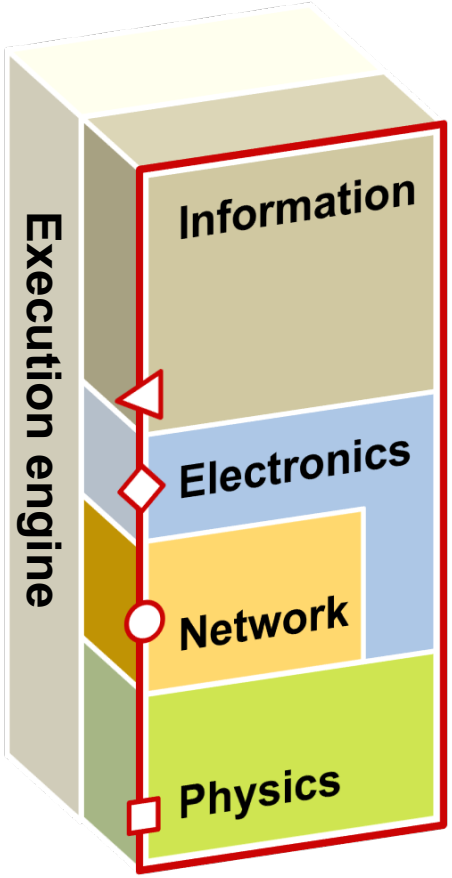
Design of heterogeneous systems

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

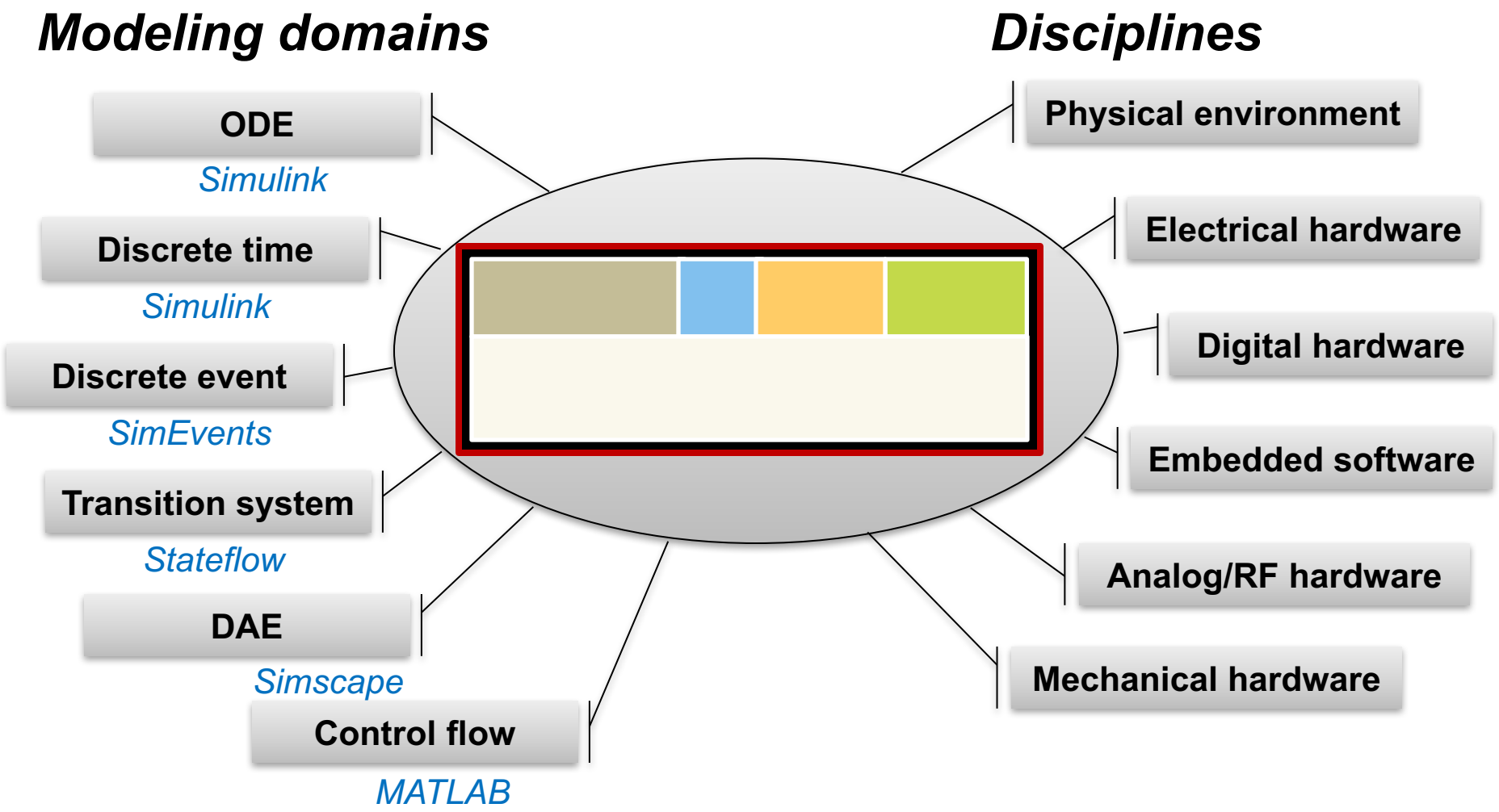


Design of heterogeneous systems

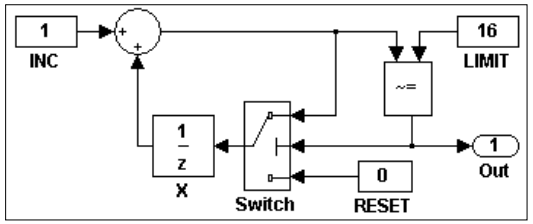
- Executable models
  - Quick feedback on design options
  - Automate design tasks
  - Automate synthesis tasks
  - …
- Computational semantics
- Execution engine
  - Combines many formalisms



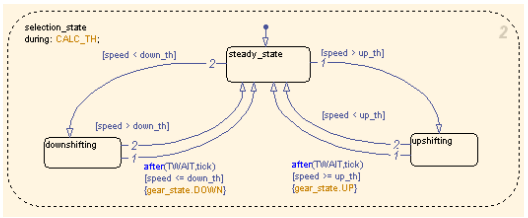
Heterogeneity in computational solutions



Code Generation: Multi-Language Support



Simulink



Stateflow

```
for n = 1:length(rxsig)
    u = rxsig(n);  % received sample
    y = conj(weights) * u;
    if n<=length(train)
        d = train(n);
    else
        d = detect(real(y)) + 1j*detect(imag(y));
    end
    % Single-tap RLS
    Delta = 1/(lambda/Delta + u*conj(u));
```

MATLAB

Unified code generation

- C Code
- C++ Code
- HDL Code
- PLC Code

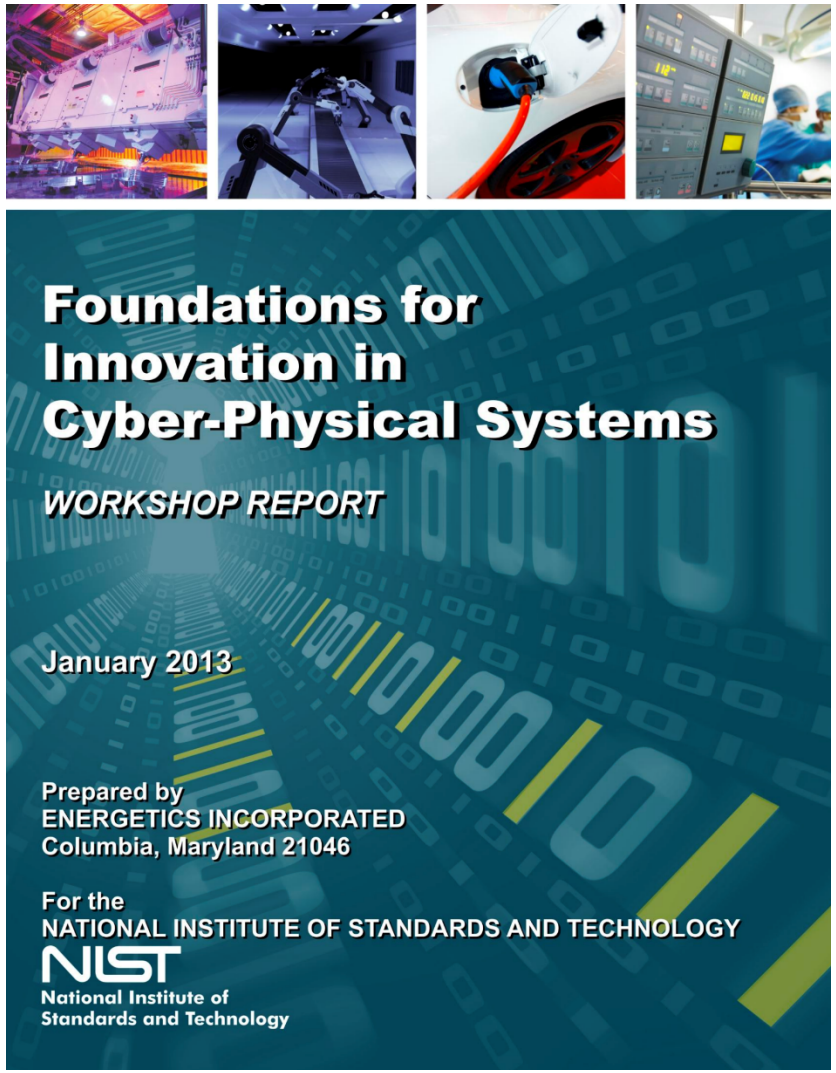
MATLAB to CUDA compiler: beta program
www.mathworks.com/matlab-cuda-beta

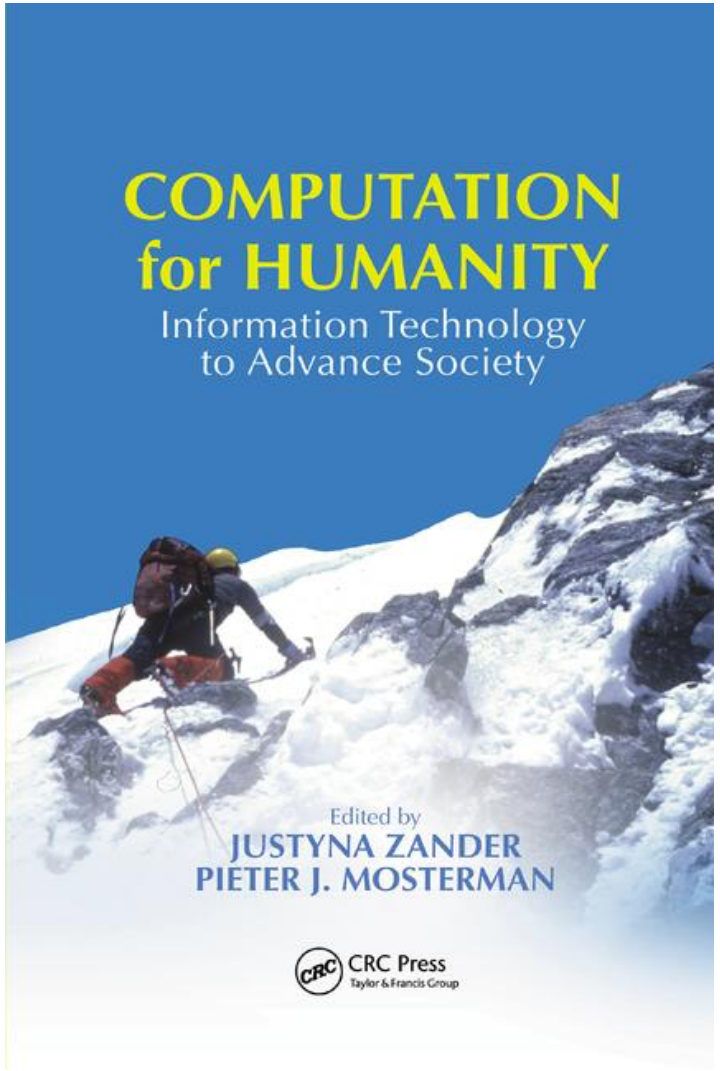
Challenges

- 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

Figure 3. Concise SERS vision slide.

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





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

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

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

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

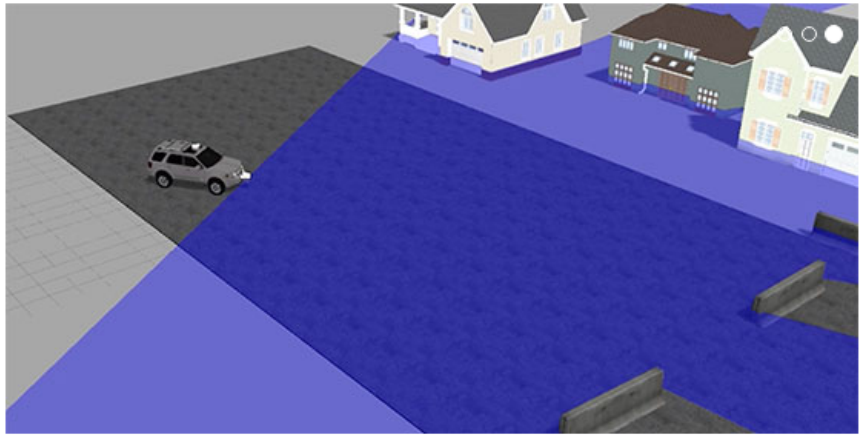
Academia

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

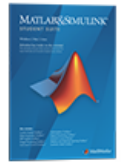
» Generating Code from a ROS Simulink Model

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

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

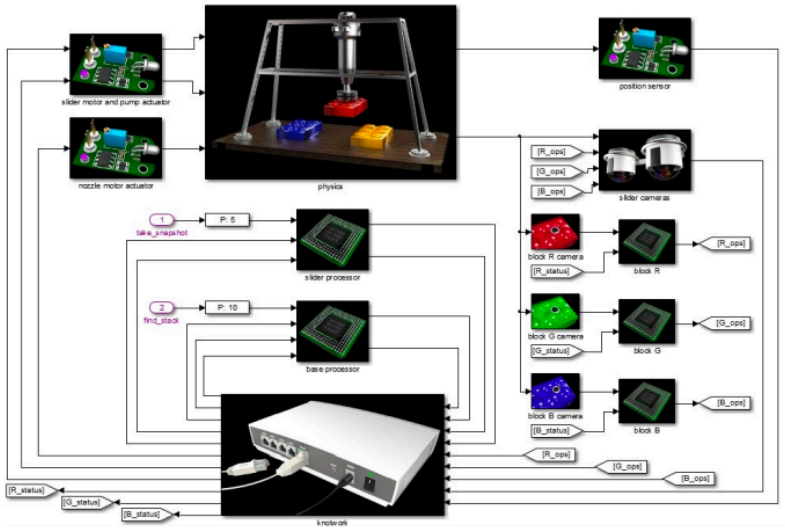


Fig. 2. Simulink® Model of the Distributed Towers of Hanoi

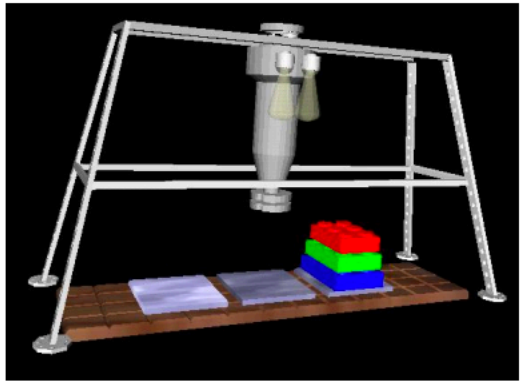


Fig. 3. The Synthesized Towers of Hanoi Scene

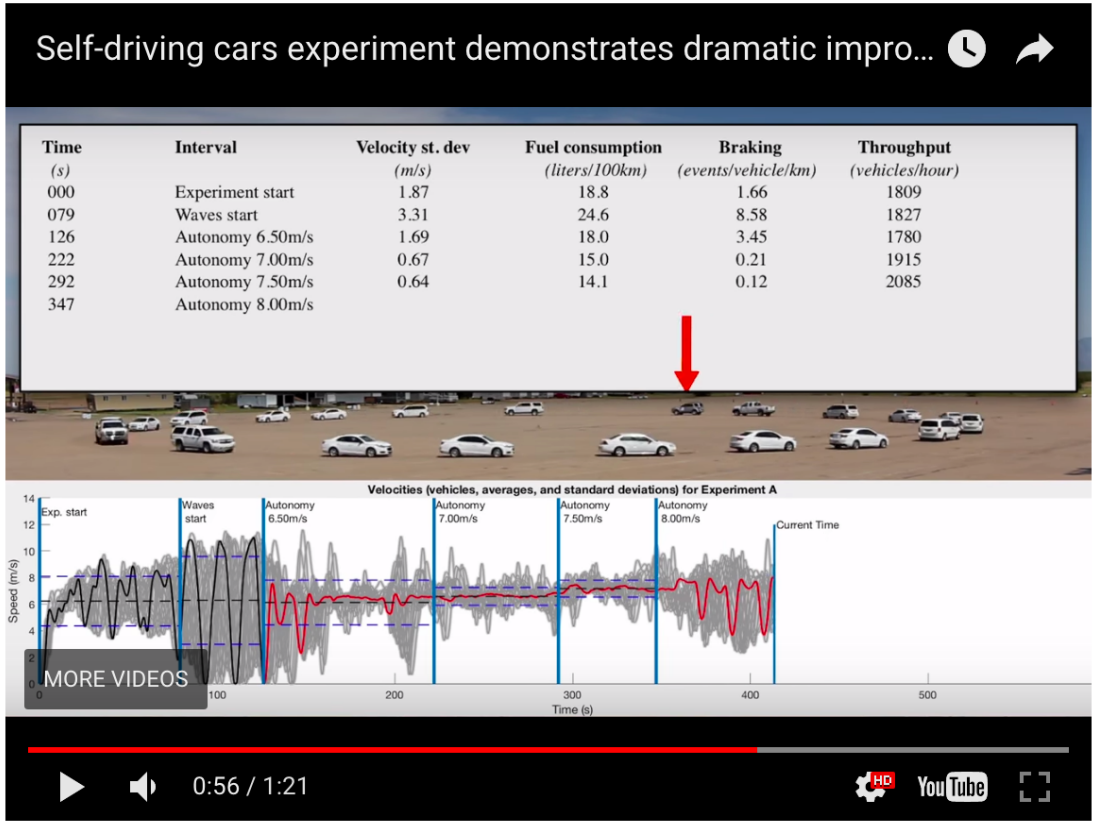
Opportunities

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

Opportunity for a transformative impact at a societal-scale!


MathWorks®
Accelerating the pace of engineering and science