KENNESAW STATE
UNIVERSITY

Module 1:

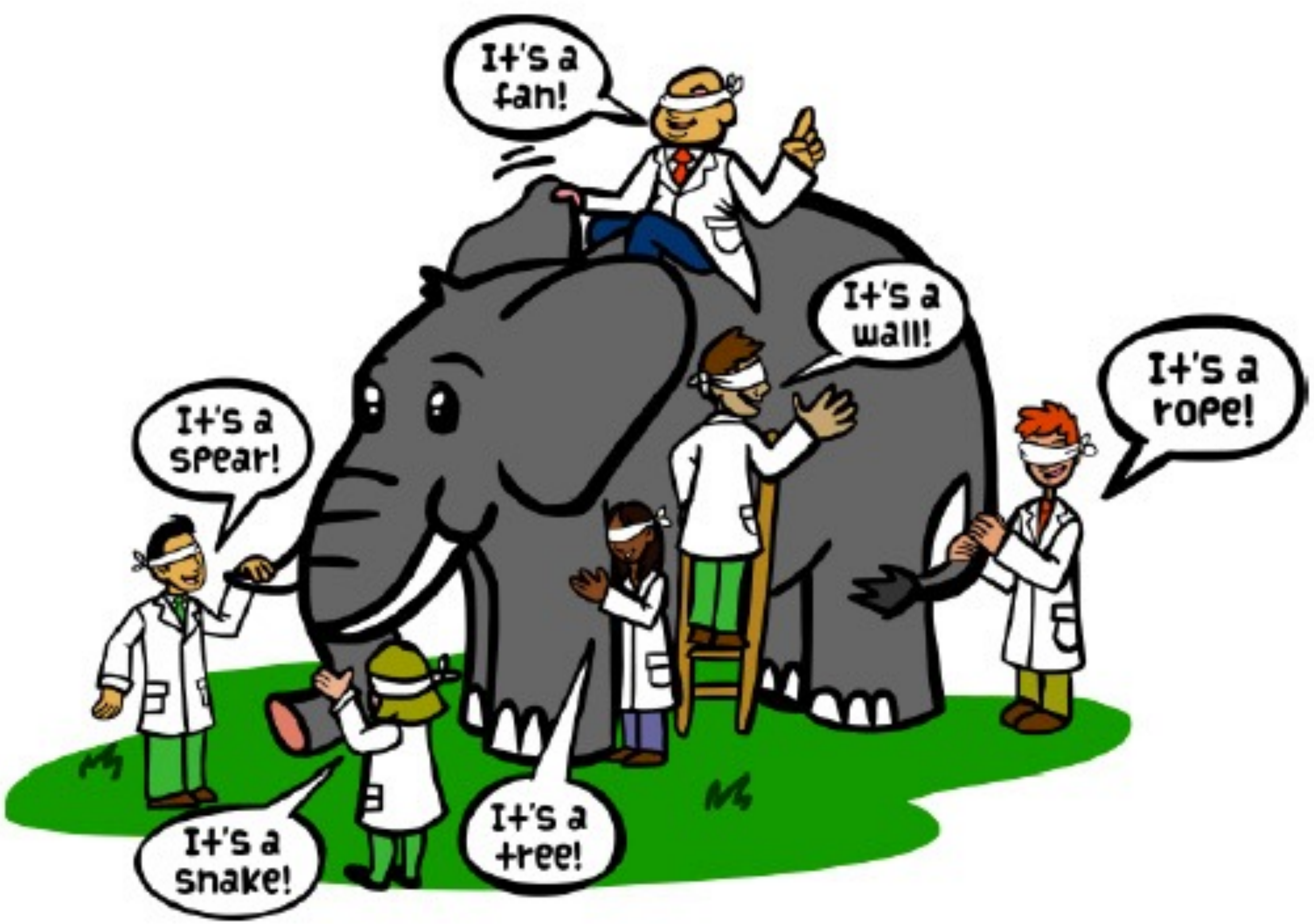
Overview of Physical IT Systems

Dr. Maria Valero

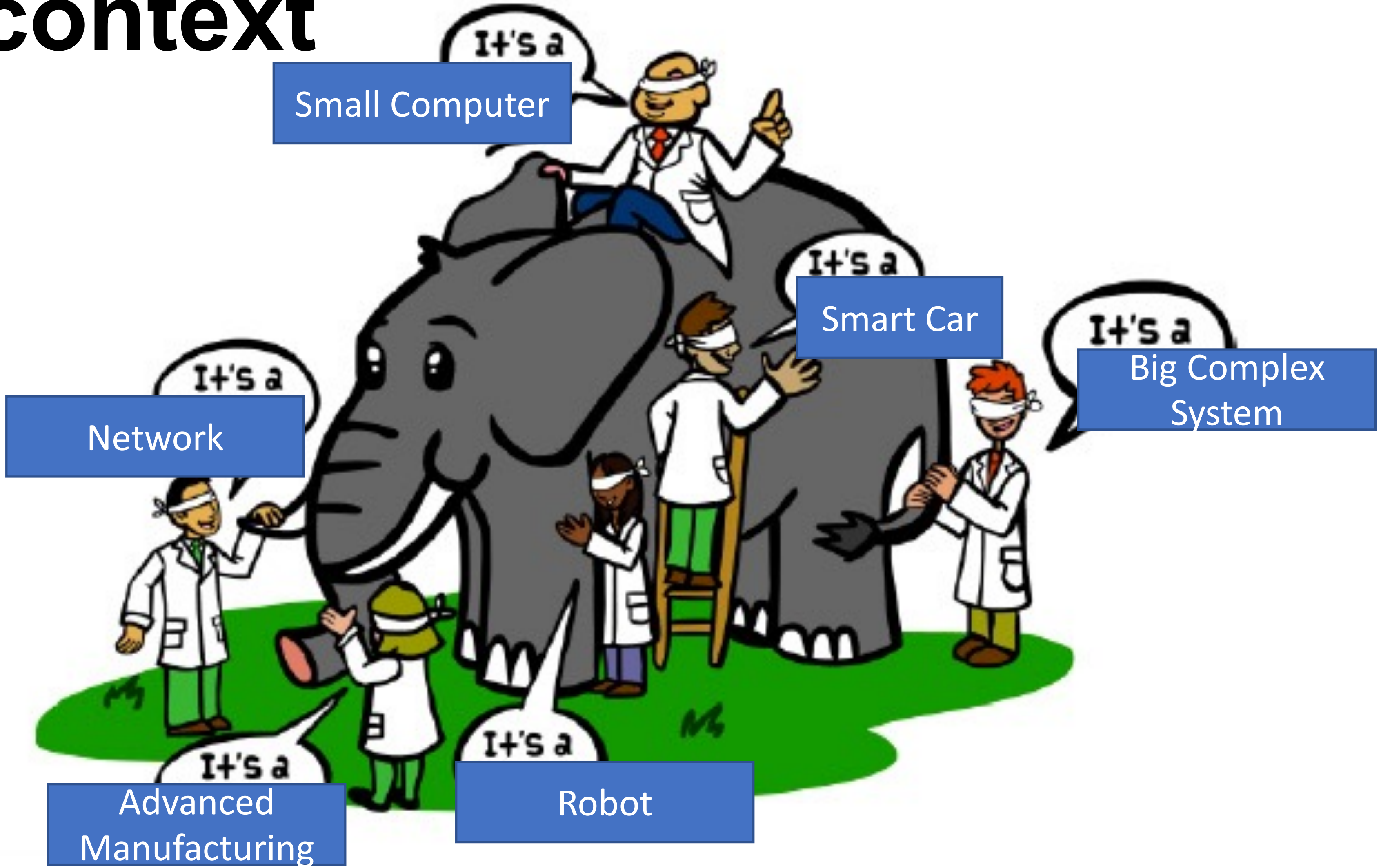
Objectives

- Understanding Cyber-Physical Systems (CPS)
- CPS Concept
- Application Domains
- Contradictions in CPS
- CPS and IoT
- Concerns in CPS

Understanding Cyber-Physical Systems

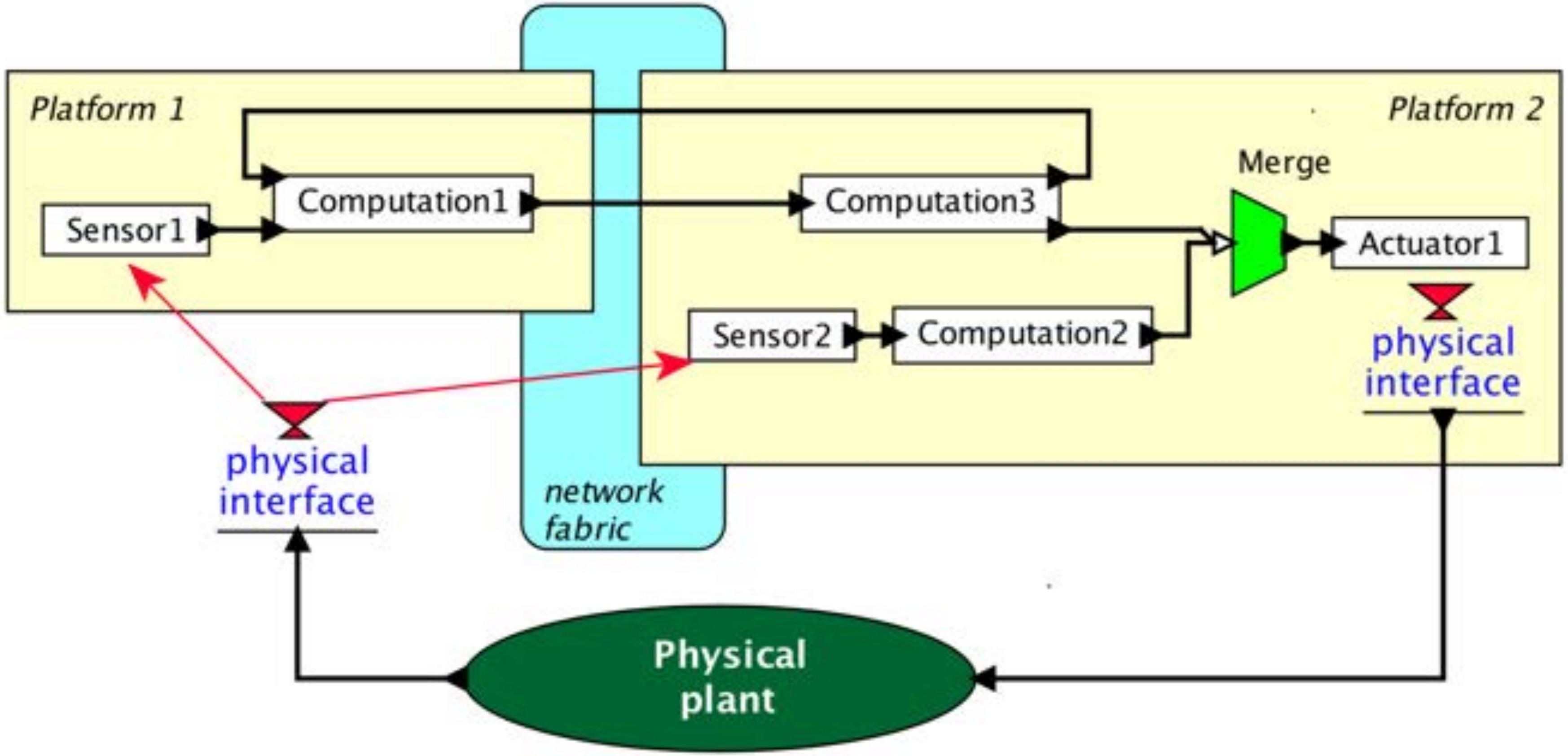


Understanding Cyber-Physical Systems in our context



About the Term

- The term "Cyber-Physical Systems" emerged in 2006, coined by Helen Gill at the National Science Foundation (NSF) in the U.S.



NSF Definition of CPS

- Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the ***seamless integration*** of computation and physical components.
- Advances in CPS will *enable* capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these critical systems.
- CPS technologies ***are transforming the way people interact*** with engineered systems, just as the Internet has transformed the way people interact with information.

Application Domains – societal impact

- Agriculture, Aeronautics, Building design, Civil infrastructure, energy, environmental quality, healthcare and personalized medicine, Manufacturing, and transportation.




CPS

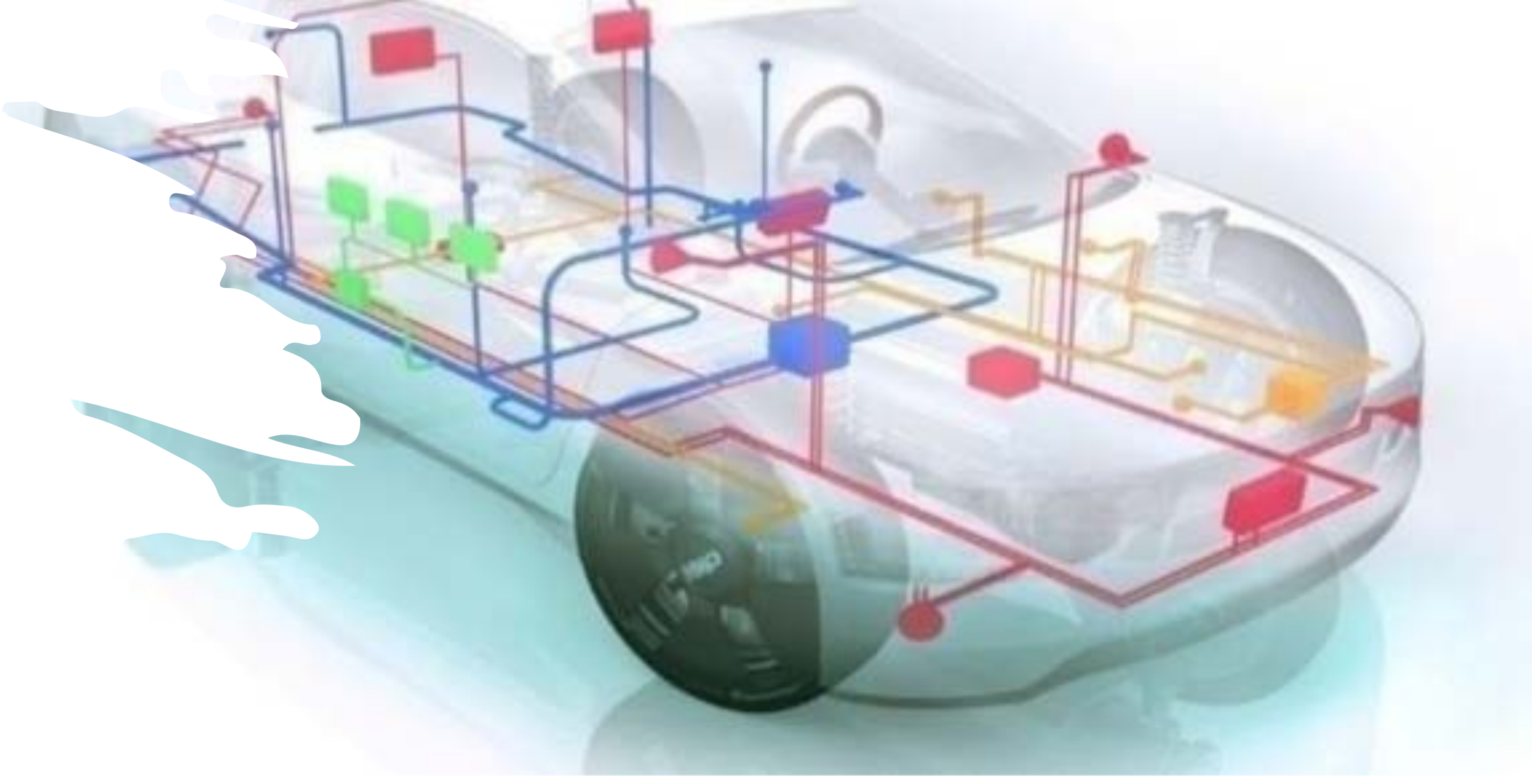
- Cyber + Physical
- Computation + Dynamics + Communication
- Security + Safety

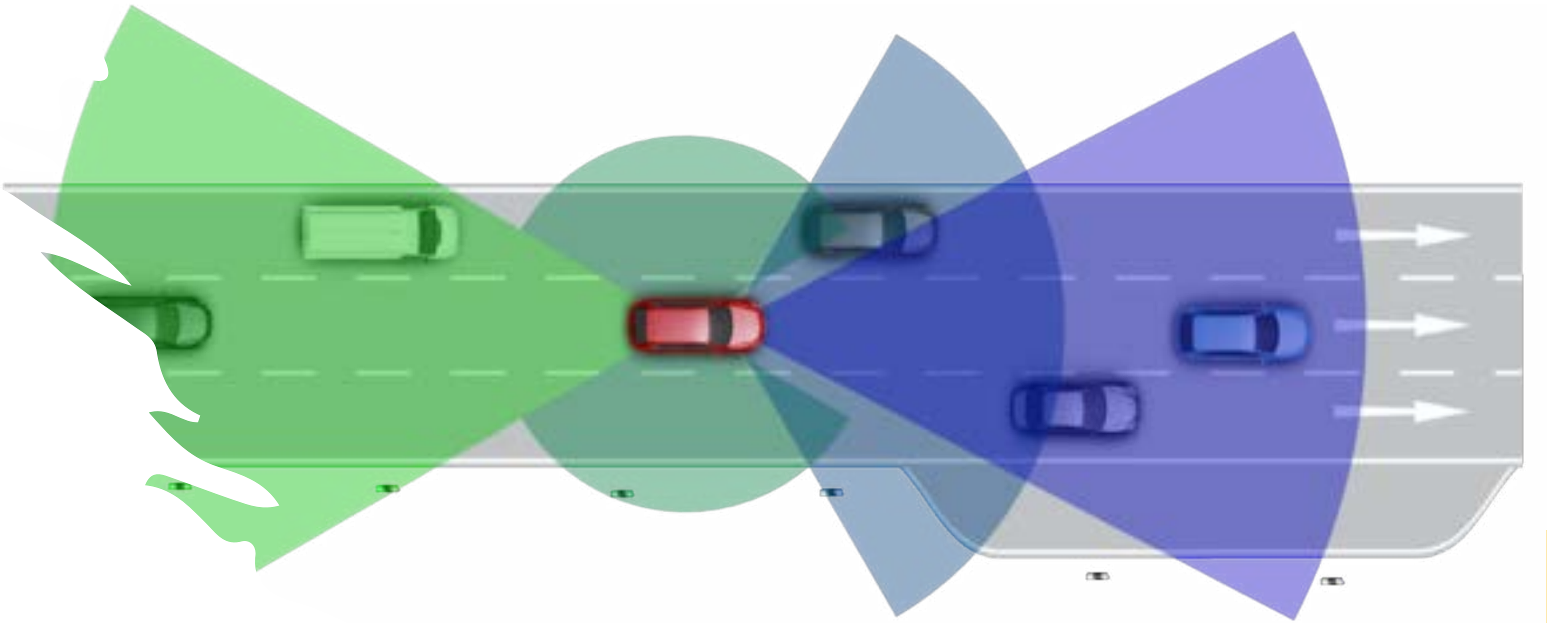

Contradictions in CPS

- Adaptability vs. Repeatability
- High connectivity vs. Security and Privacy
- High performance vs. Low Energy
- Asynchrony vs. Coordination/Cooperation
- Scalability vs. Reliability and Predictability
- Laws and Regulations vs. Technical Possibilities
- Economies of scale (cloud) vs. Locality (fog)
- Open vs. Proprietary
- Algorithms vs. Dynamics

Automotive CPS

- Safer Transportation
- Reduced Emissions
- Smart Transportation
- Energy efficiency
- Climate Change
- Human-Robot collaboration



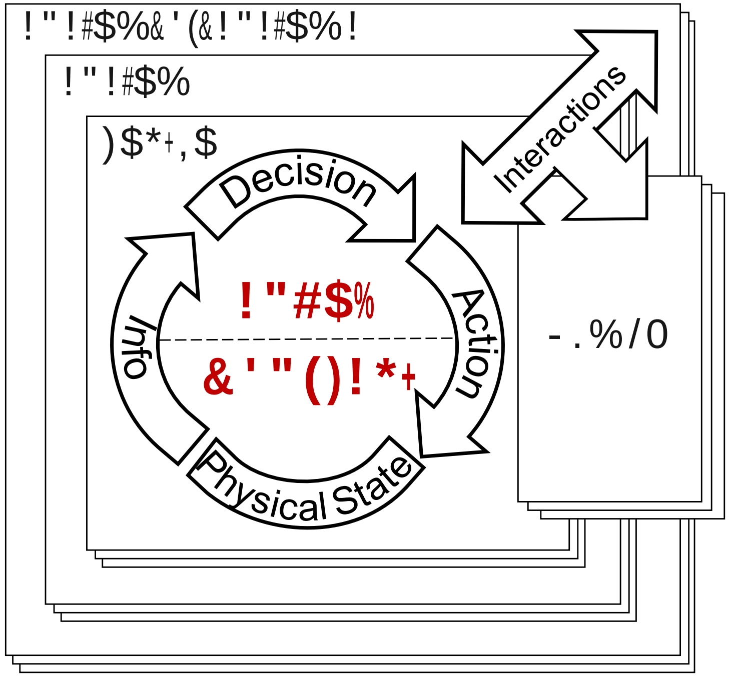


Example of CPS System

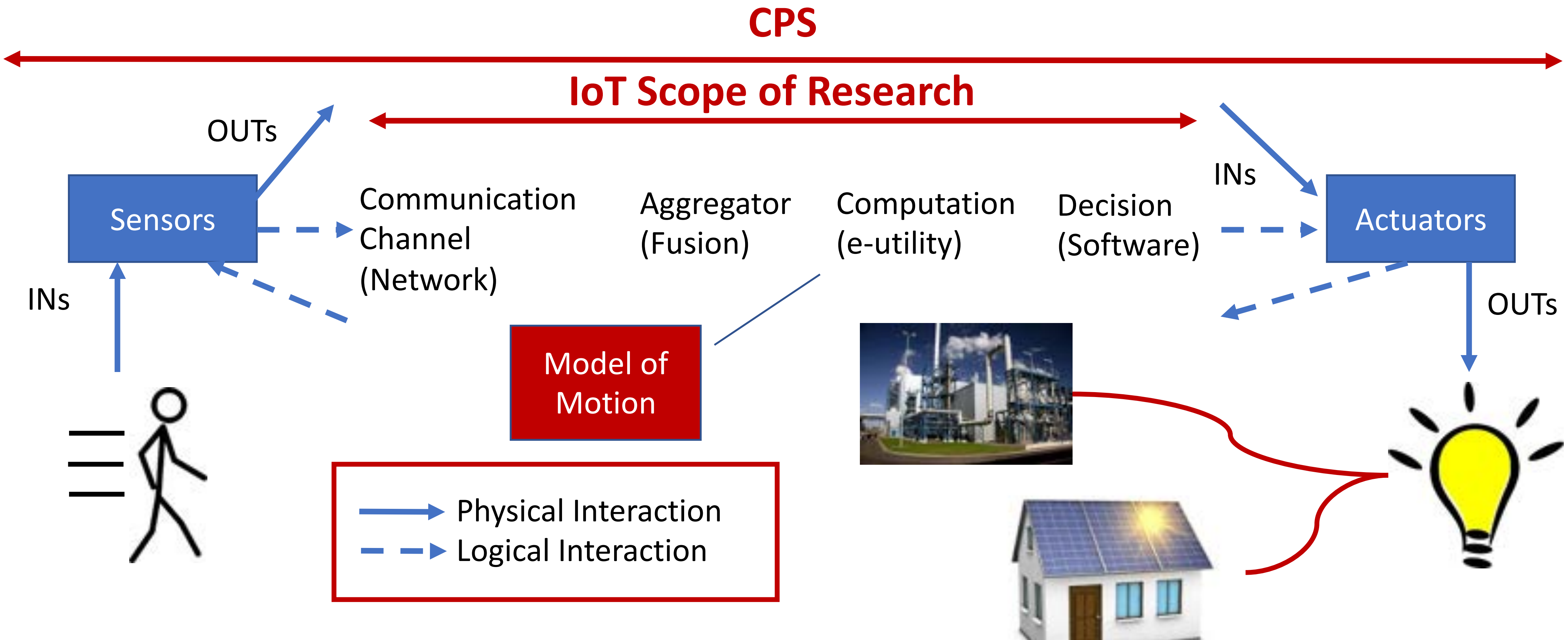
- STARMAC Quadrotor Aircraft

CPS and IoT

- **Cyber-Physical Systems (CPS)** comprise interacting with physical IoT devices
- Examples
  - Smart Spoon enabling Parkinson’s patients to feed themselves (see https://www.liftware.com/)
  - Autonomous vehicle operating without wired or wireless connections outside the vehicle, e.g.
    - a Mars rover operating between messages from Earth
    - the original vehicles in the first DARPA Challenge
    - cruise missile/smart bomb in flight to target



CPS vs. IoT: Motion Activated Light



Framework Schema: **Phys-Log-Log-Log-Log-Phys**
Testbed: **Experiment, Measurement and Assurance**
Challenges: **Interoperability, Composition and Composition Types, Trustworthiness, etc.**

IT- vs CPS-Based Risk Mitigation

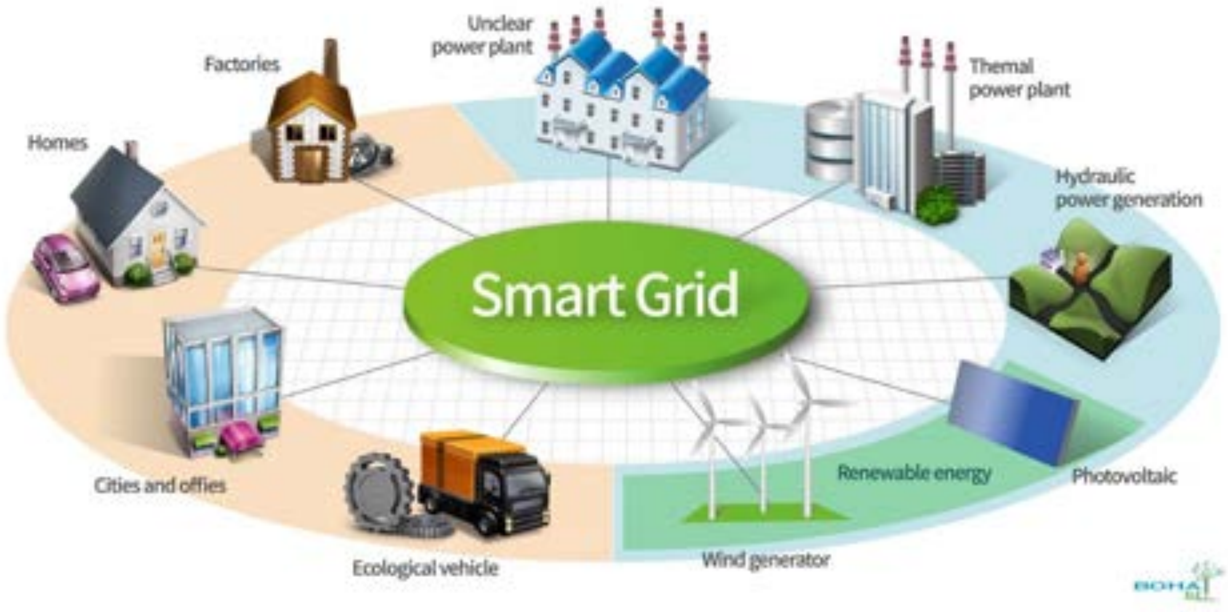
	Primary Impact of Failure		Mitigation Mechanisms		
	Digital	Physical	Digital	Analog	Physical
IT System	✓		✓		
IoT/CPS	✓	✓	✓	✓	✓

"Better cybersecurity through physics!"

Potential Concerns in CPS

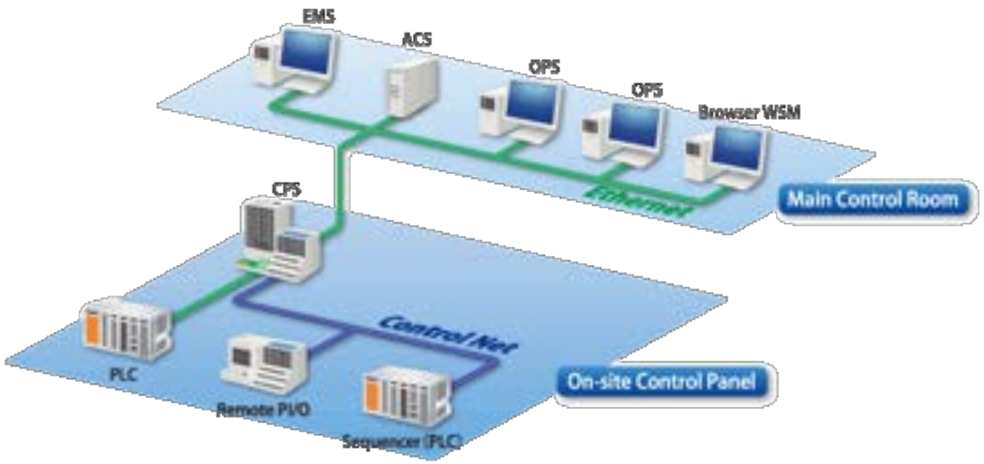
CPS Vulnerability

- Are your energy, healthcare, water, shipping, transportation systems vulnerable to network attacks?
- What, if any, are the vulnerabilities in such systems?
- When exploited, how might such vulnerabilities affect people?



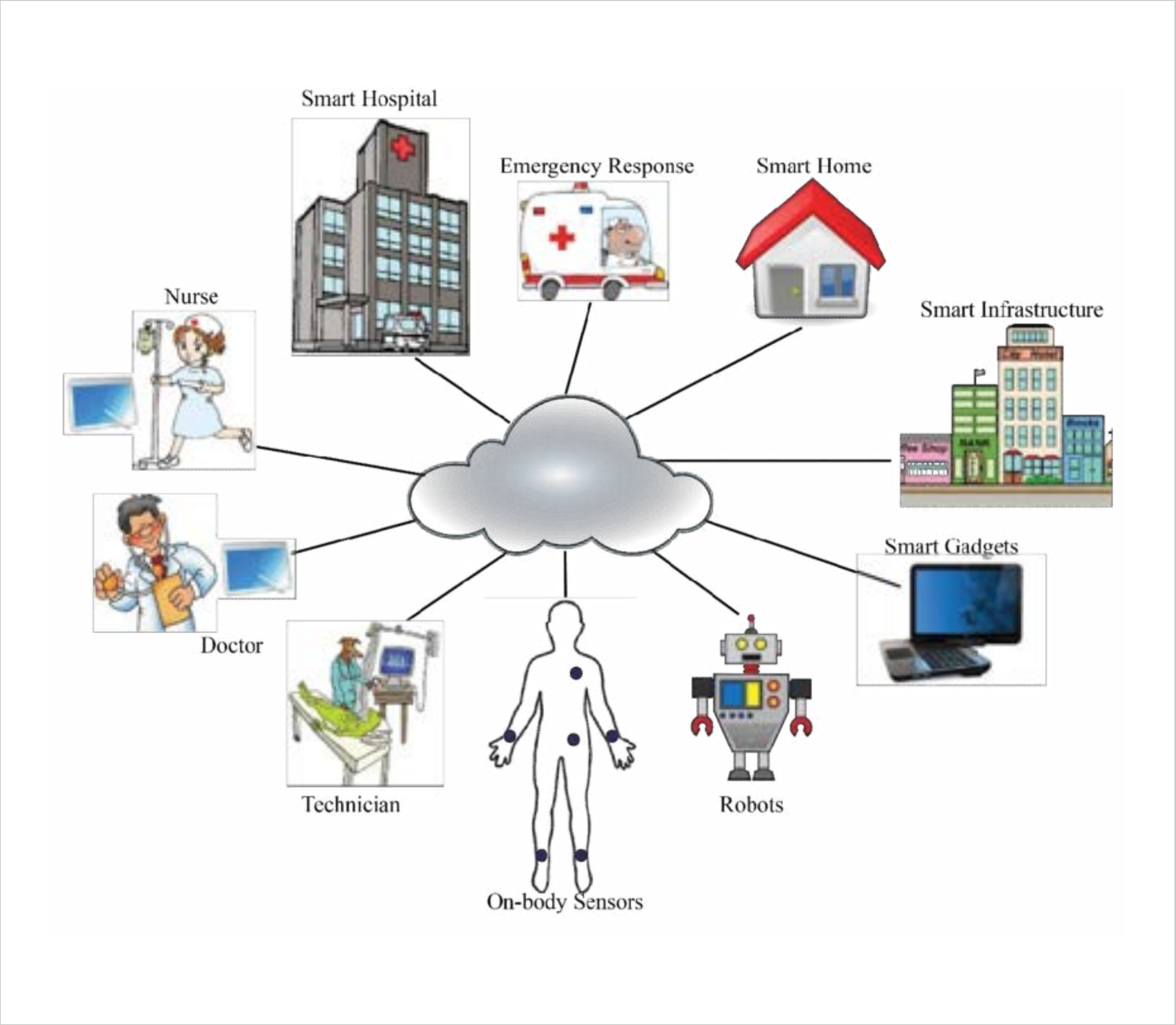
CPS Control systems

- Are the control systems in your large and critical CPSs systems robust enough to withstand deception attacks?
- Are these control systems programmed to withstand denial of service attacks?



Surviving Physical Attacks

- What happens if we lose part, or even most of the computing systems?
- Will redundancy alone solve the problem?
- How to measure and quantify of resilience of current systems?
- How to ensure high availability of CPS?



Defending Against Device Capture Attack

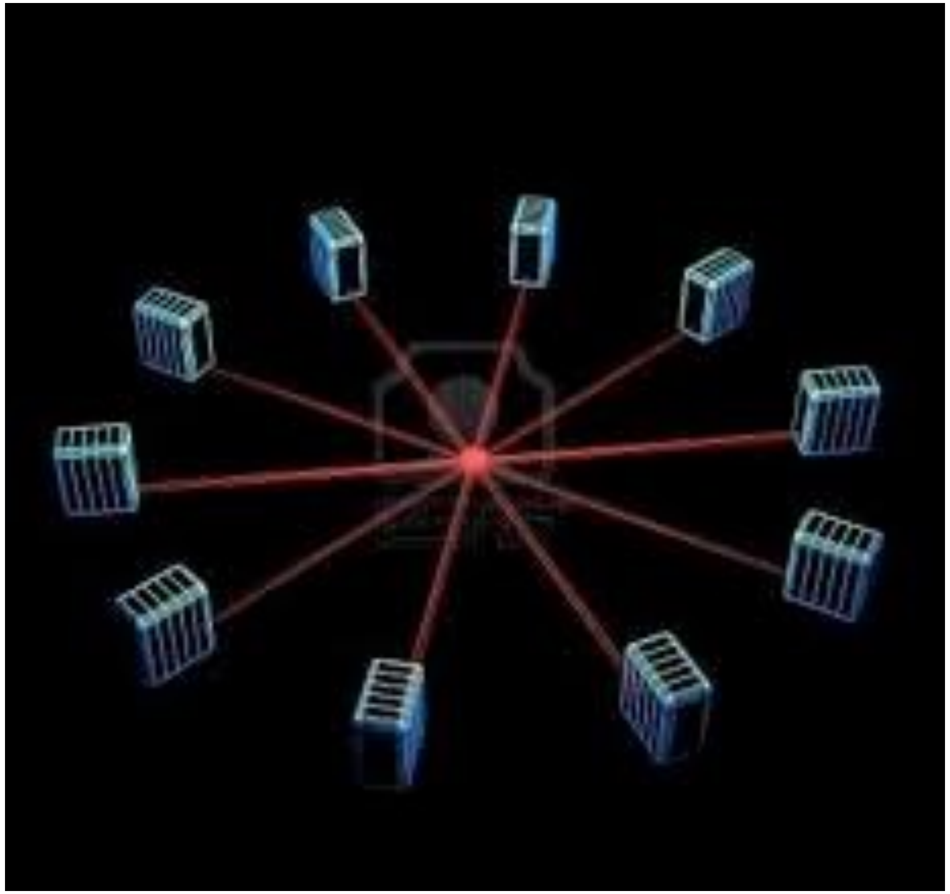
- Physical devices in CPS systems may be captured, compromised and released back by adversaries.
- How to identify and ameliorate the system damage with trusted hardware but potentially untrusted/modified software?


Real-Time Security in CPS

- CPS often requires real-time responses to physical processes
- Little Study on how attacks affect the real-time properties of CPS
- How to guarantee real-time requirements under attack?

Concurrency in CPS

- CPS is concurrent in nature, running both cyber and physical processes
- Little research on handling large-scale concurrent systems



Collaboration and Isolation

- CPS needs to effectively isolate attackers while maintaining collaborations among different, distributed system components
- How to avoid cascading failures while minimizing system performance degradation?