Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 1: Introduction to CPS

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

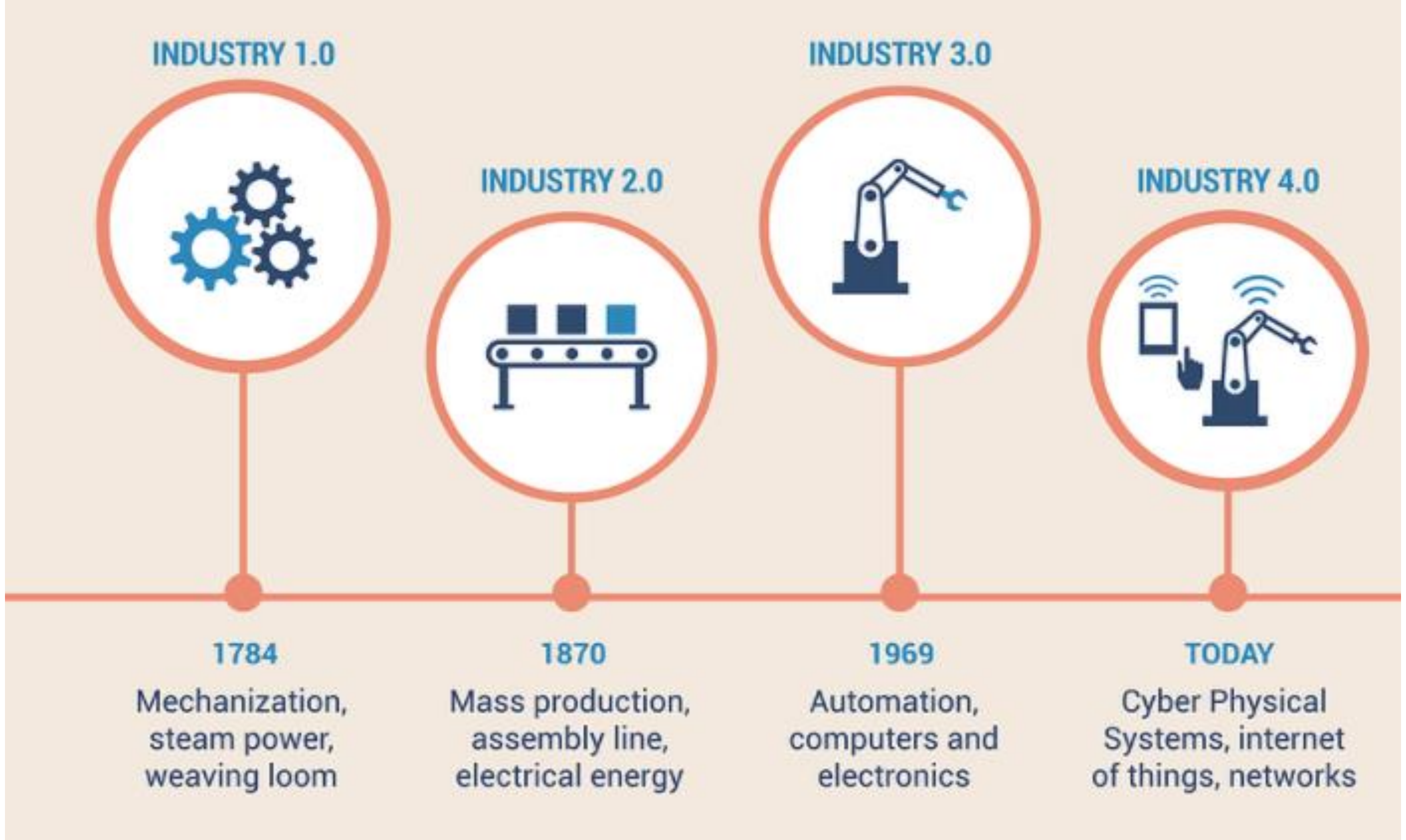
What is CPS

Architecture of CPS

CPS use cases

Why CPS security even matters

Industrial Evolution



INDUSTRY 1.0

1784

Mechanization, steam power, weaving loom

INDUSTRY 2.0

1870

Mass production, assembly line, electrical energy

INDUSTRY 3.0

1969

Automation, computers and electronics

INDUSTRY 4.0

TODAY

Cyber Physical Systems, internet of things, networks

Cyber Physical System

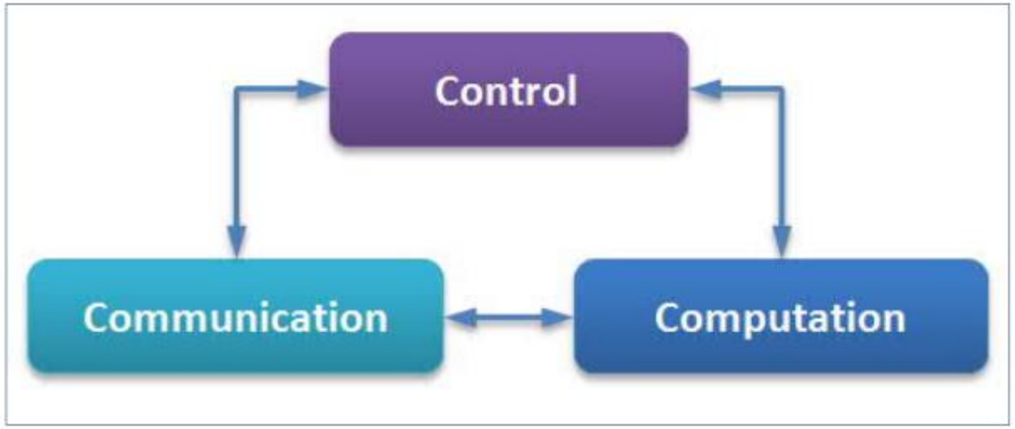
Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the **seamless integration** of computation and physical components.

CPS technologies are transforming the way people interact with engineered systems,

- just as the Internet has transformed the way people interact with information.

Cyber-physical systems integrate;

- sensing, computation, control and networking into physical objects and infrastructure,
- connecting them to the Internet and to each other



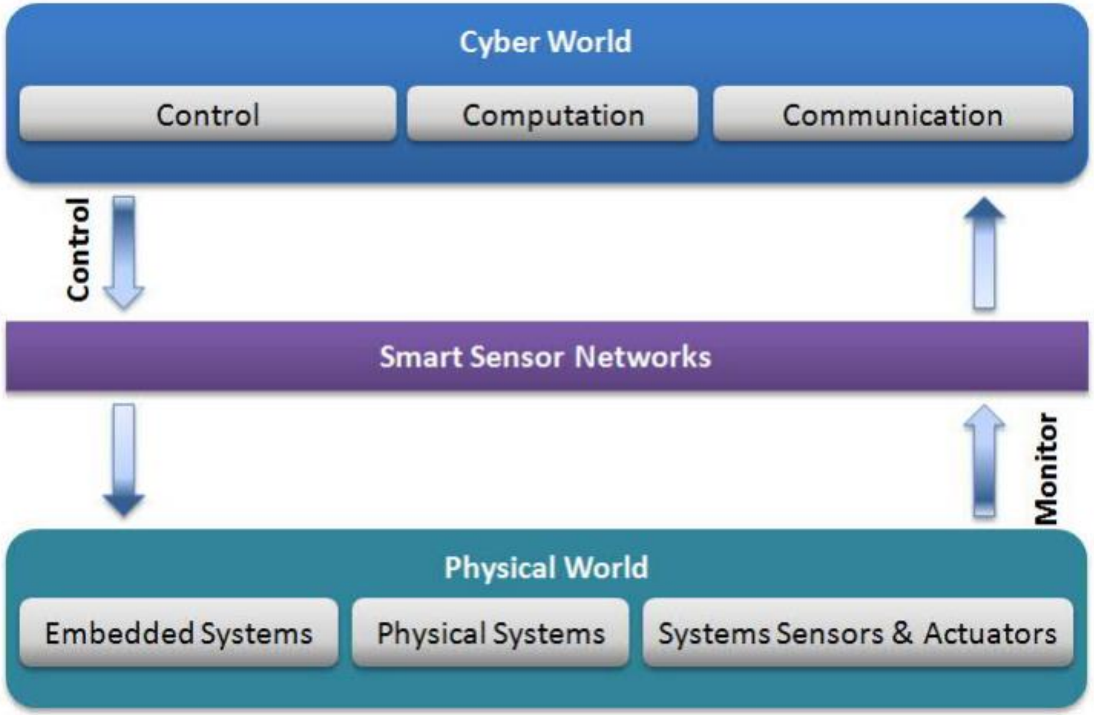
Minimal requirements a for a cyber physical system

Cyber Physical System

NIST: CPS comprises interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

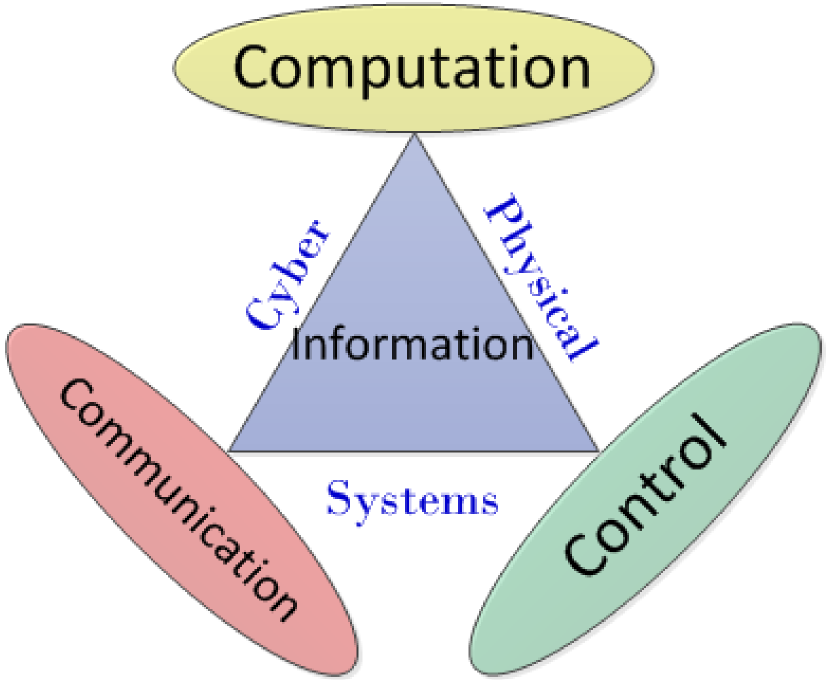
- These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.
- Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, etc.

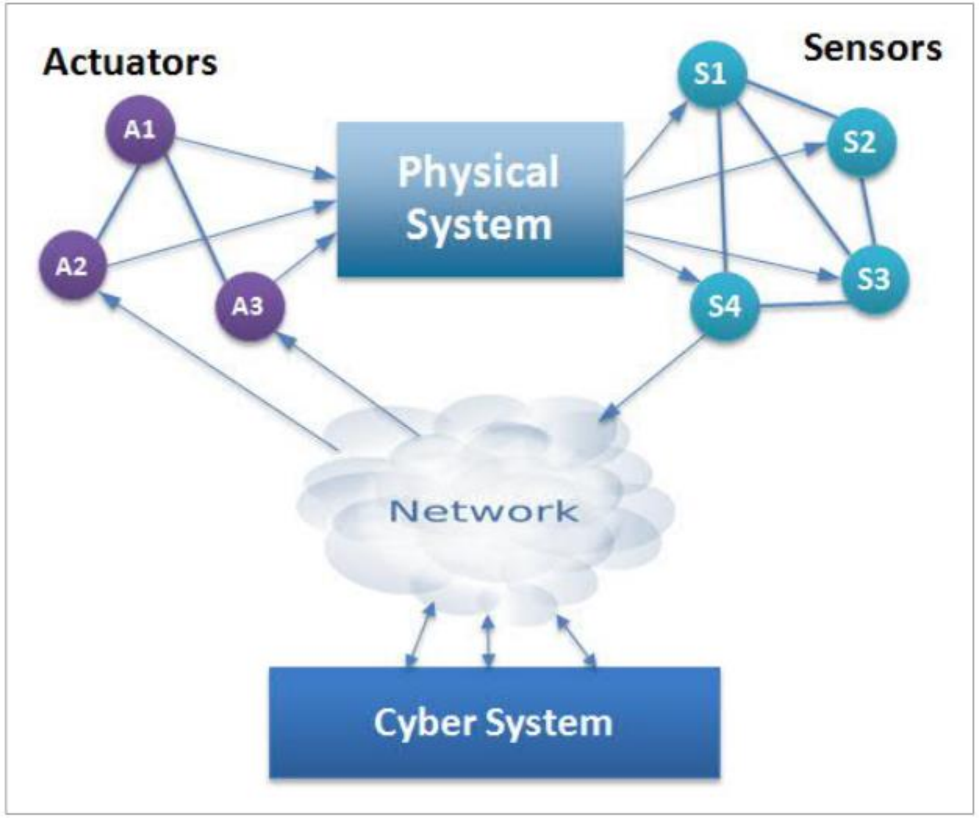
Enabling a smart and connected world



Main building blocks of a cyber physical system

Parts of CPS

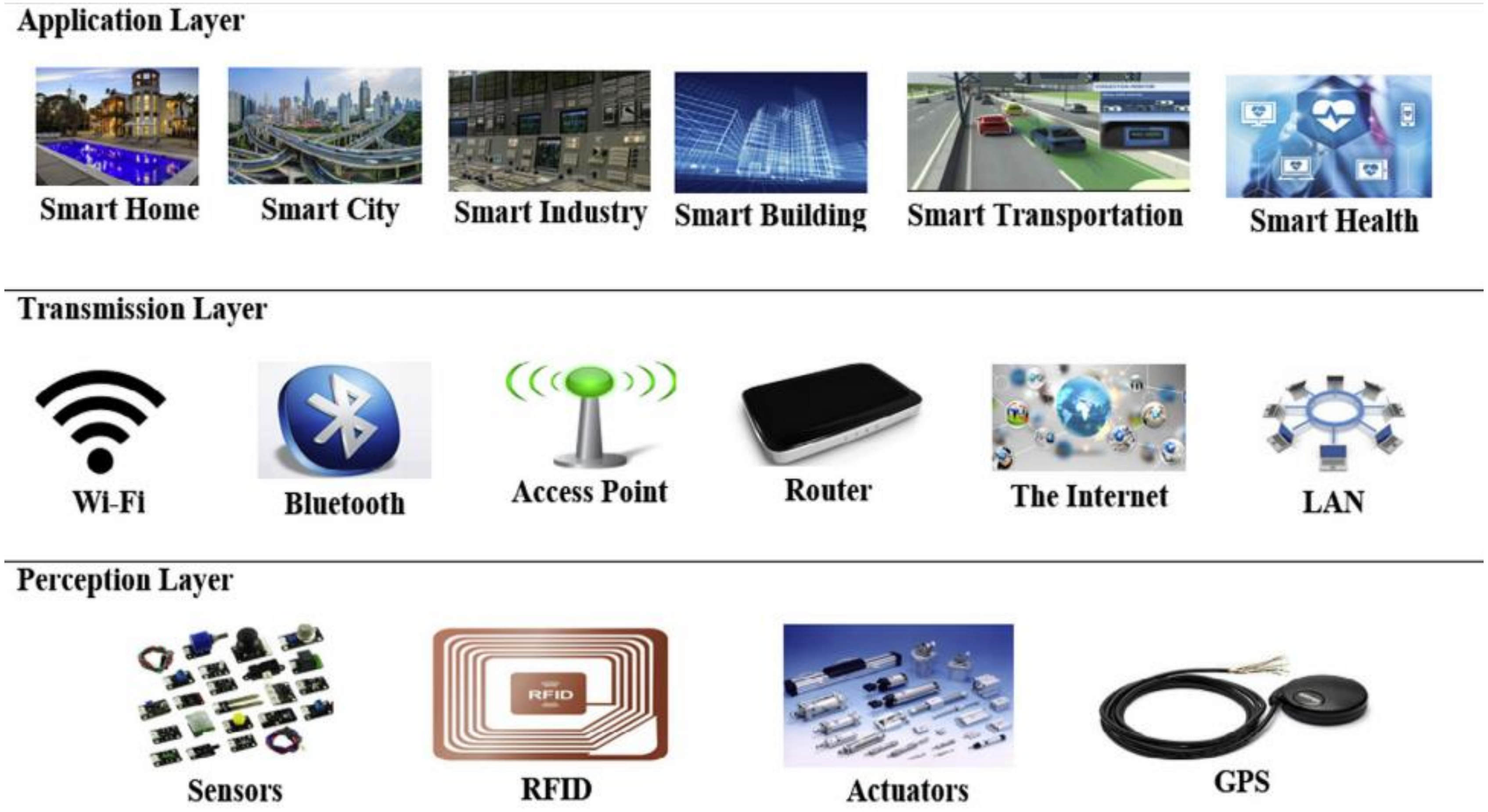




Generic Architecture of Cyber Physical Systems

CPS Architecture

Typical three layers cyber-physical system



CPS in Bigger Picture

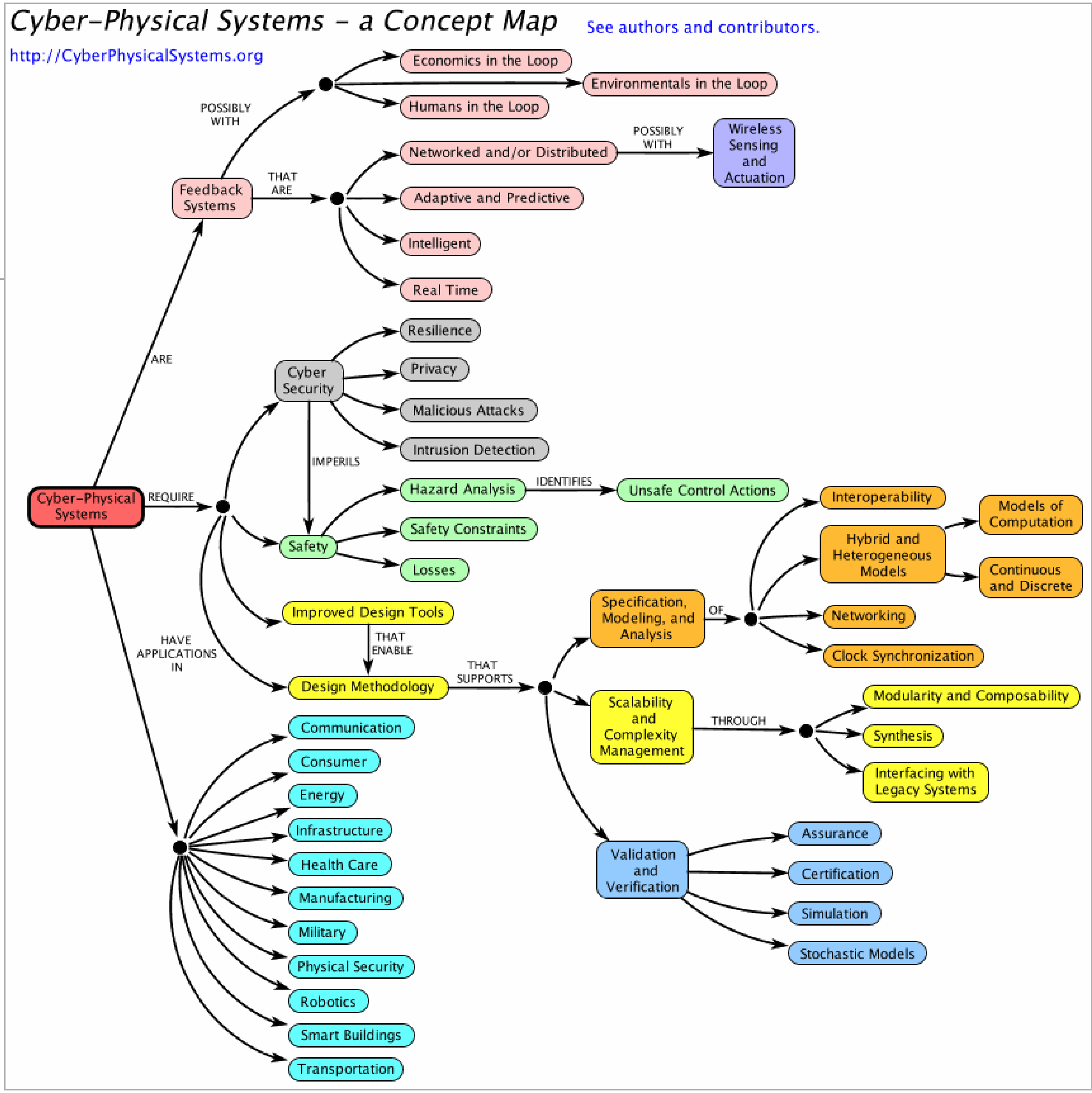
Are Feedback Systems

Require;

- Cyber security
- Safety
- Design Methodology and Tools

Applications in

- Energy
- Transportation, etc.



Cyber-Physical Systems – a Concept Map

See authors and contributors.

http://CyberPhysicalSystems.org

Cyber-Physical Systems ARE Feedback Systems

Feedback Systems POSSIBLY WITH: Economics in the Loop; Environmentals in the Loop; Humans in the Loop

Feedback Systems THAT ARE: Networked and/or Distributed; Adaptive and Predictive; Intelligent; Real Time

Networked and/or Distributed POSSIBLY WITH Wireless Sensing and Actuation

Cyber-Physical Systems REQUIRE: Cyber Security; Safety; Improved Design Tools; Design Methodology

Cyber Security: Resilience; Privacy; Malicious Attacks; Intrusion Detection

Cyber Security IMPERILS Safety

Safety: Hazard Analysis; Safety Constraints; Losses

Hazard Analysis IDENTIFIES Unsafe Control Actions

Improved Design Tools THAT ENABLE Design Methodology

Design Methodology THAT SUPPORTS: Specification, Modeling, and Analysis; Scalability and Complexity Management; Validation and Verification

Specification, Modeling, and Analysis OF: Interoperability; Hybrid and Heterogeneous Models; Networking; Clock Synchronization

Hybrid and Heterogeneous Models: Models of Computation; Continuous and Discrete

Scalability and Complexity Management THROUGH: Modularity and Composability; Synthesis; Interfacing with Legacy Systems

Validation and Verification: Assurance; Certification; Simulation; Stochastic Models

Cyber-Physical Systems HAVE APPLICATIONS IN: Communication; Consumer; Energy; Infrastructure; Health Care; Manufacturing; Military; Physical Security; Robotics; Smart Buildings; Transportation

What ‘CPS’ include

Internet of Things (IoT)

Industrial Internet (Industrial Networks, Industrial Control Systems)

Smart Cities

Smart Grid

"Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances)

What CPSes are not

Not desktop computing

Not traditional, embedded/real-time systems

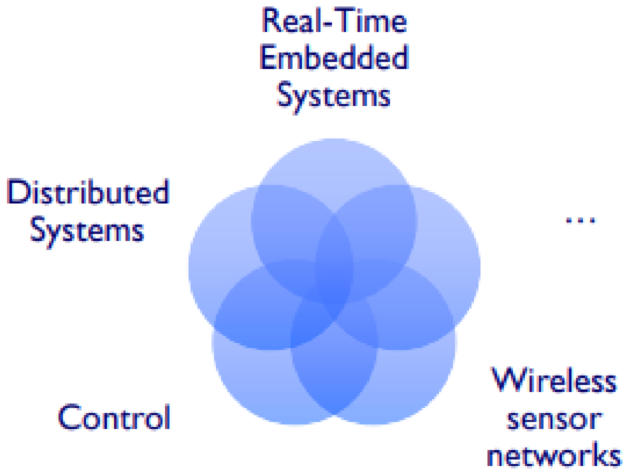
- Embedded systems still are part of CPS, a subset

Not sensor networks itself,

- Even though CPSes have sensor networks too

Not Internet of Things (IoT)

- Often used to mean CPS as well
- CPS include IoT



Characteristics of CPS

Cyber

- Cyber capability in each physical component
- Networking of the components

System of systems

- Unconventional computational and physical substrates (Bio? Nano?)

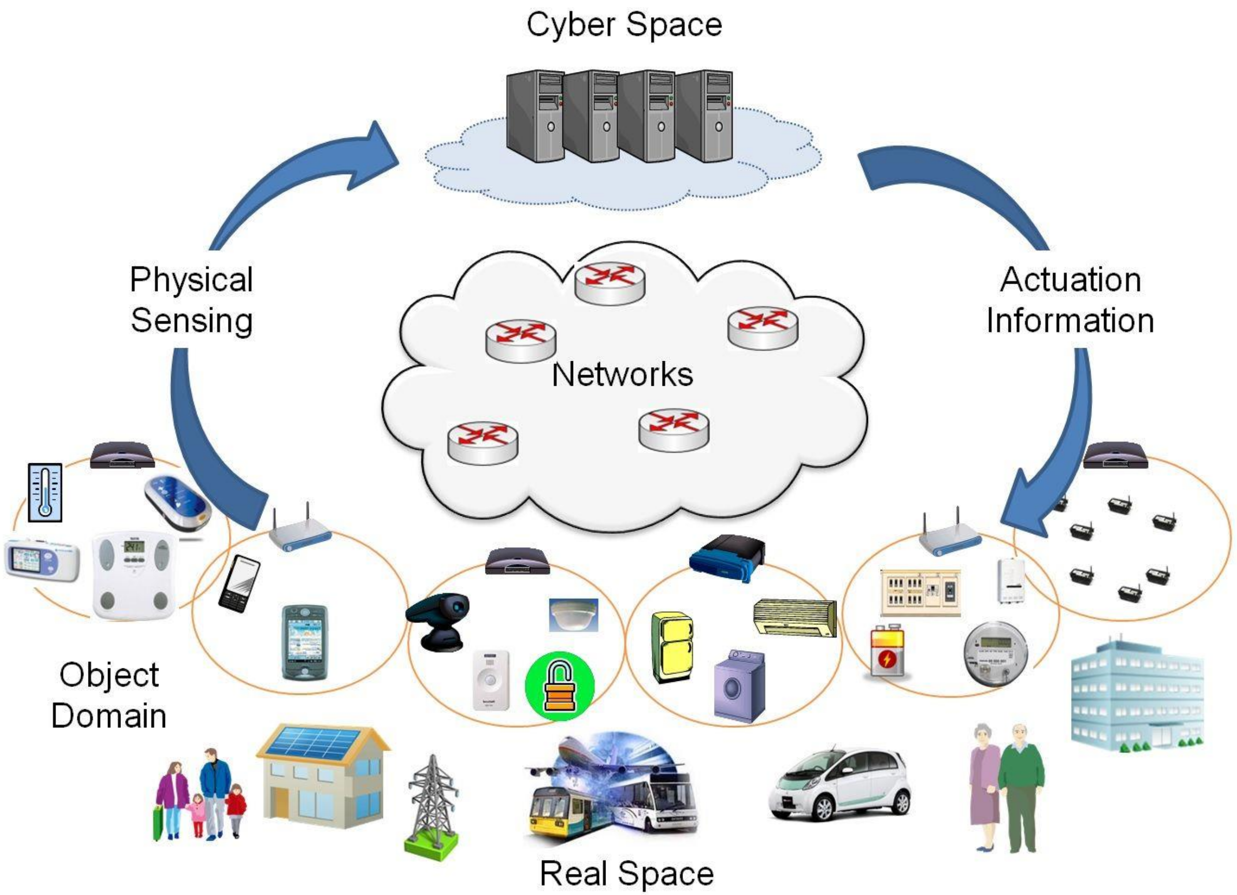
Interaction between control/computing/communication

- High degrees of automation, control loops must close at all scales

Ubiquity

- Causes security and privacy concerns

CPS Use Cases in our Lives

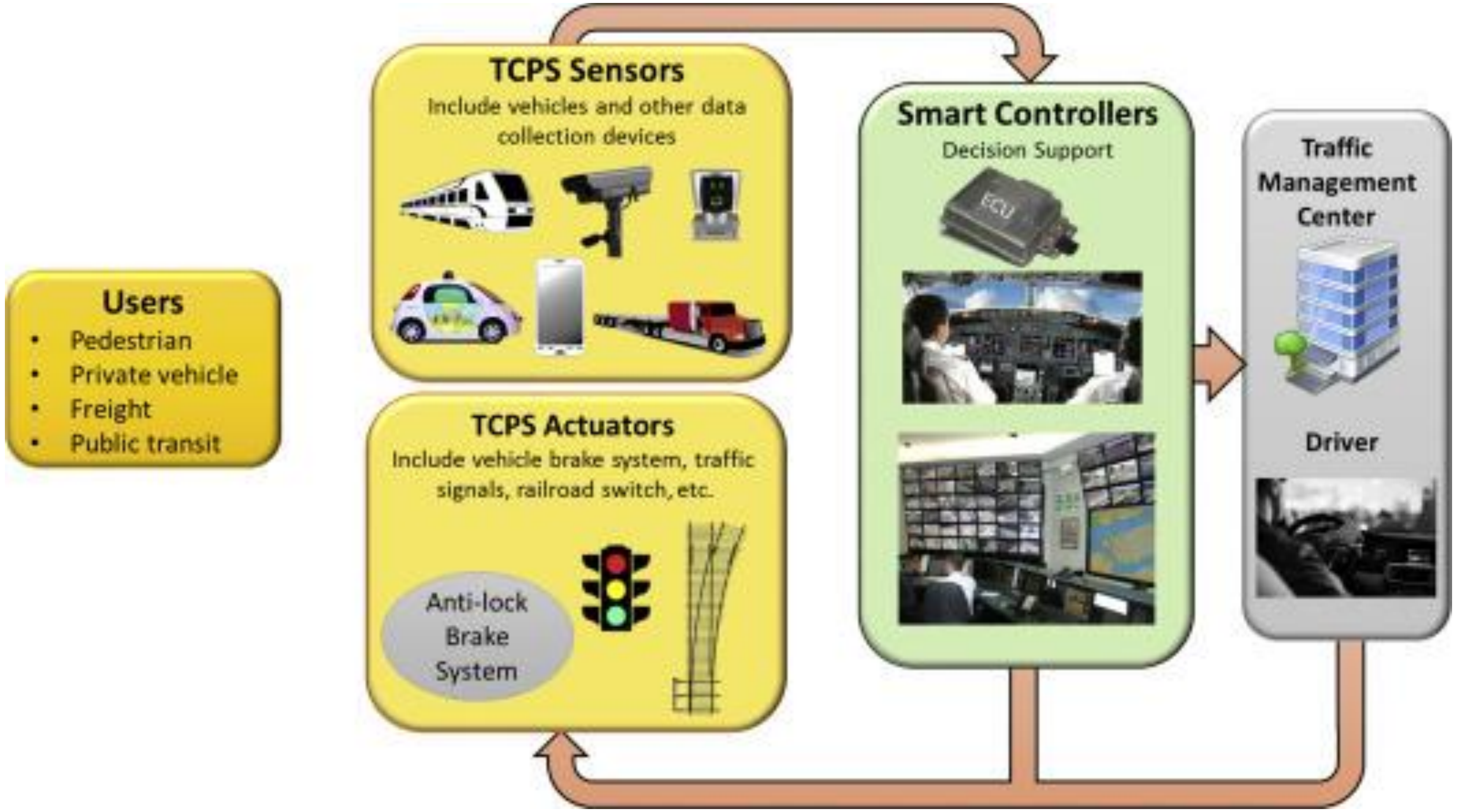


CPS Use Case Example: Transportation

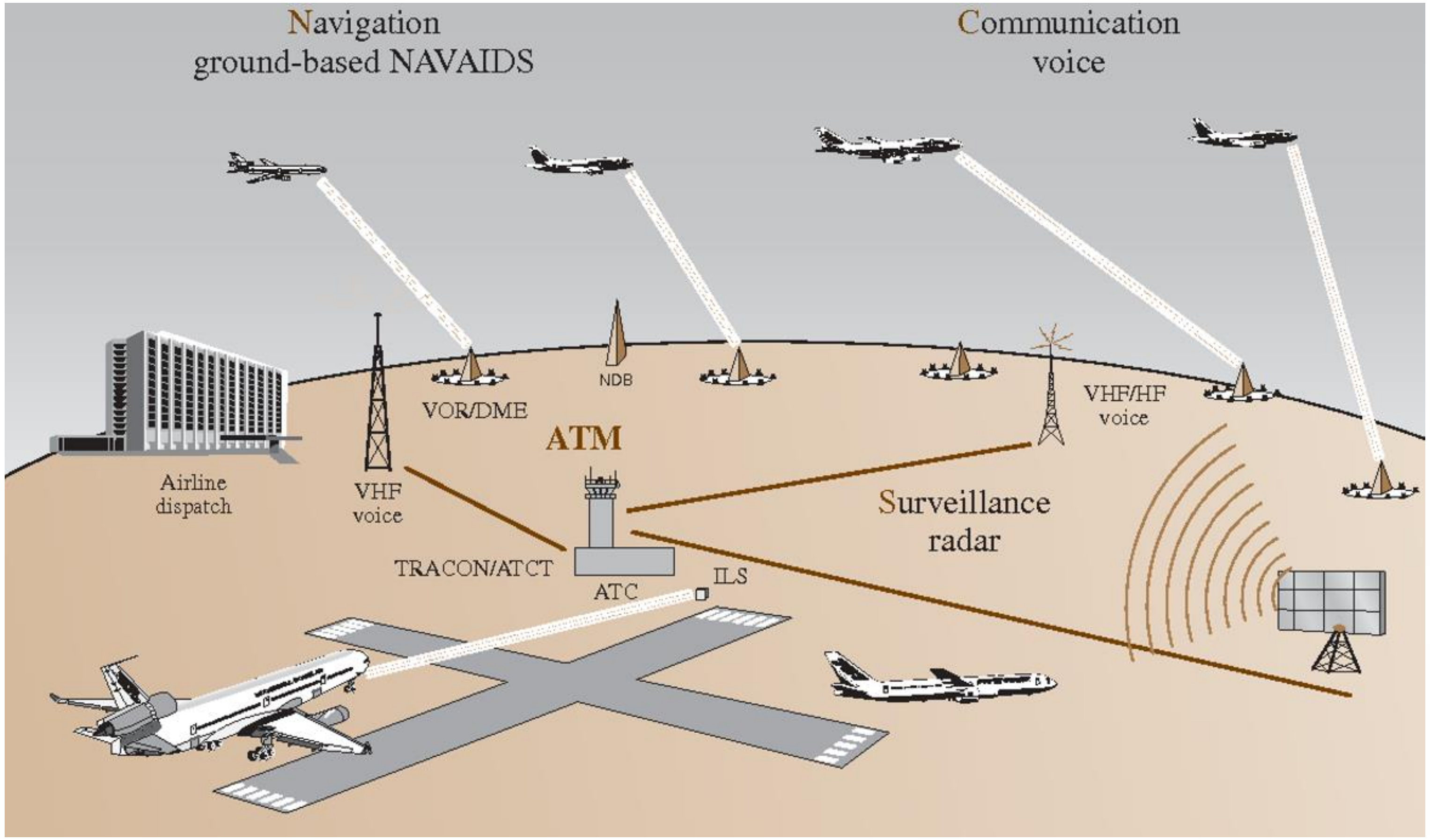
Vehicles are very digitized

- Lots of sensors to collect data
- CAN Bus for communication
- Electronic Control Unit (ECUs) to make control decisions

Physical Actions: Cruise control, breaking, lane change warning, parking, airbag control


Users
Pedestrian
Private vehicle
Freight
Public transit
TCPS Sensors
Include vehicles and other data collection devices
TCPS Actuators
Include vehicle brake system, traffic signals, railroad switch, etc.
Anti-lock Brake System
Smart Controllers
Decision Support
ECU
Traffic Management Center
Driver

Another Transportation CPS Example



CPS Use Case Example: Health care

Monitoring and control devices in health

Mobile health became a new market with our smart phones and wearable

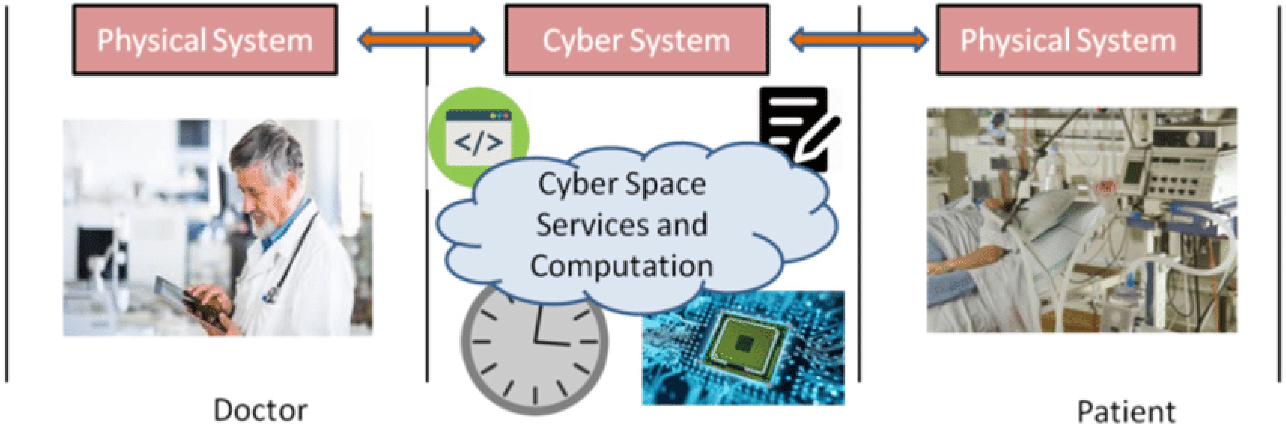
- Numerous Medical IoT devices

At the CPS side, there are also many new devices

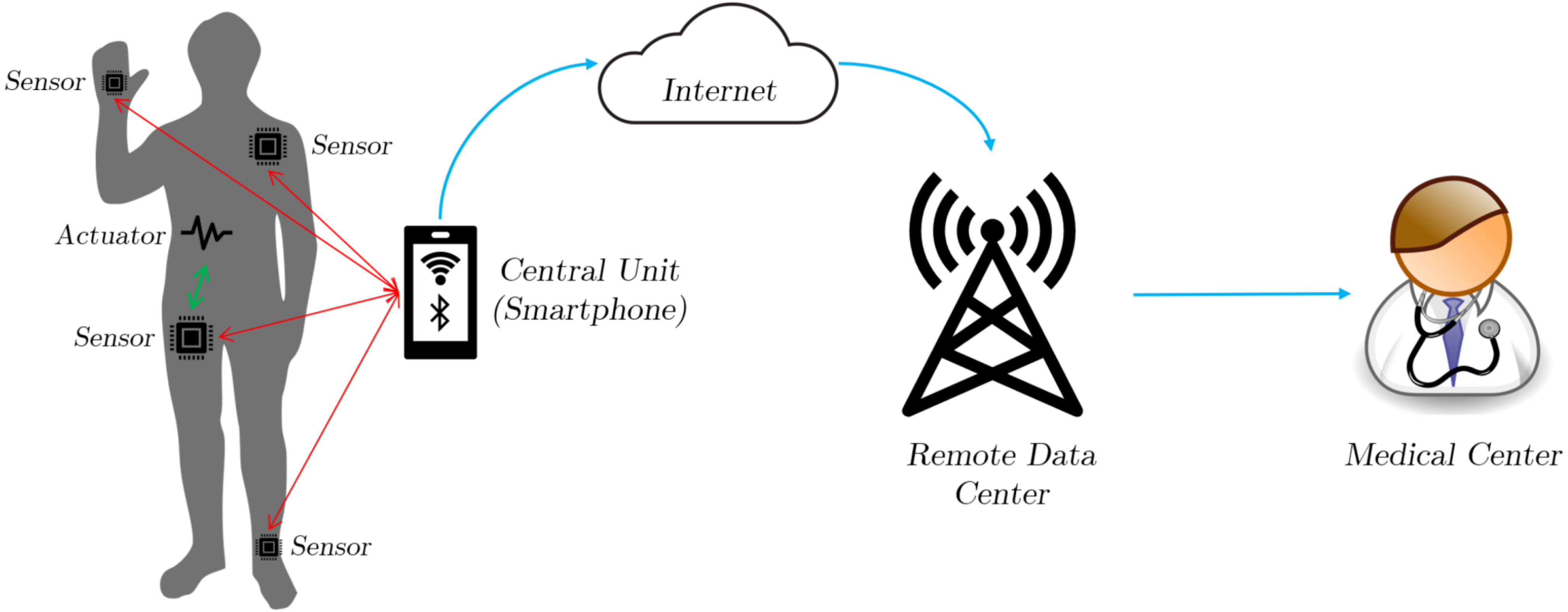
- Insulin pumps, pulse oximeters, sleep apnea devices, etc.

Telemedicine

- Remote surgery, robotic surgery
- System coordination

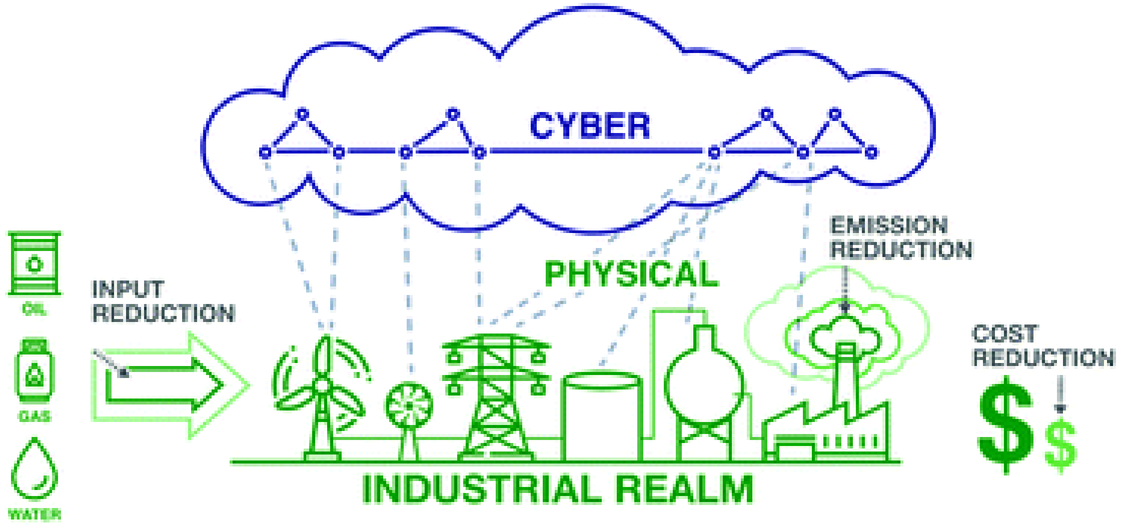


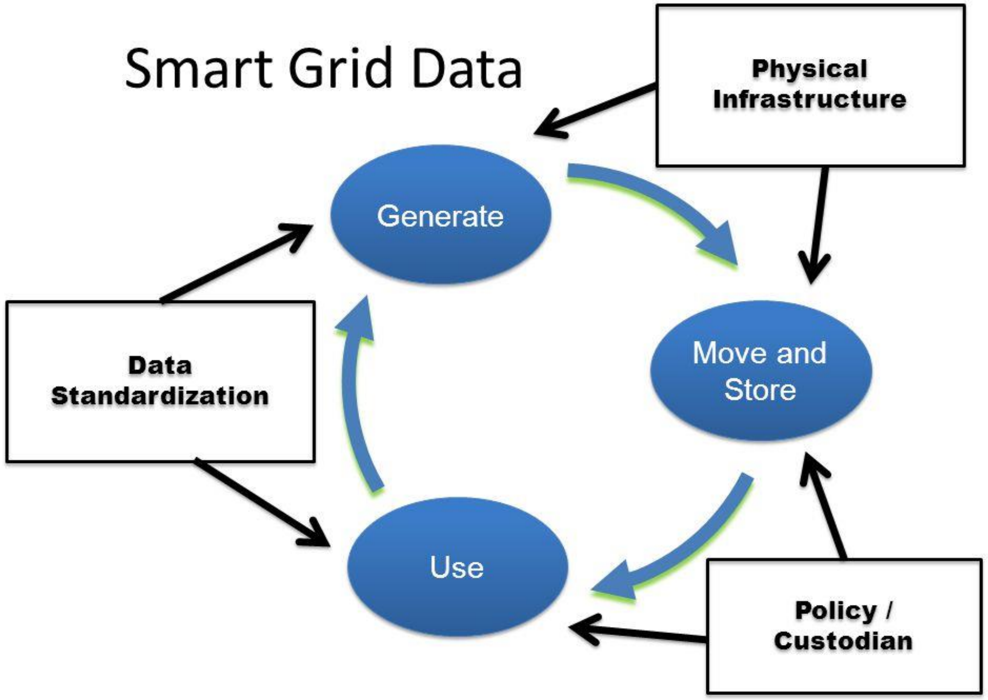
Another Health Care CPS Example



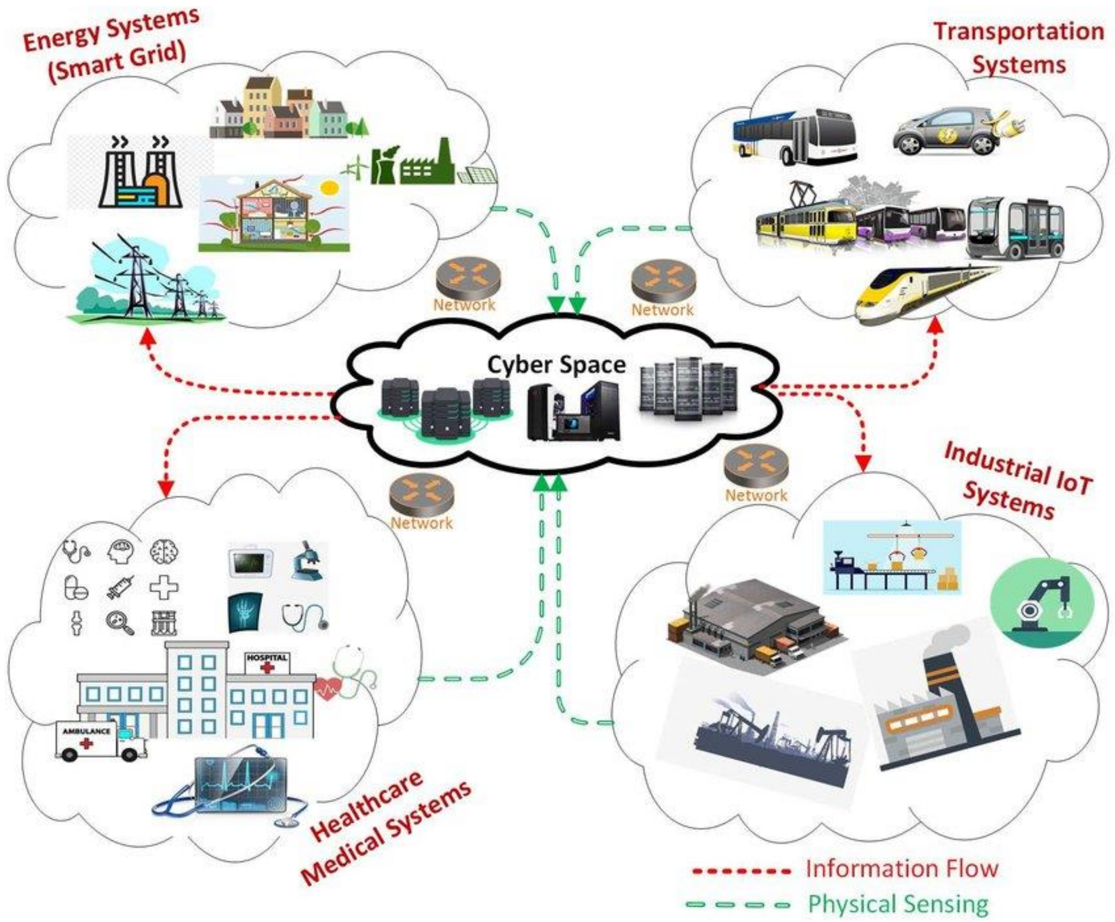
CPS Use Case Example

Power/Energy CPS:





CPS Use Cases



CPS Domain Examples

Aerospace

Agriculture

Buildings

Cities

Defense

Disaster resilience

Education

Emergency response

CPS Domain Examples

Entertainment/sports

Environmental monitoring

Financial services

Healthcare

Infrastructure (communications, power, water)

Leisure

Manufacturing

Supply chain/retail

Transportation

Weather

CPS Benefits/Social Impacts

Reduced traffic fatalities and congestion

Black-out free energy distribution

- Energy aware buildings

Location independent access to health services

- Perpetual life assistants

Self correcting infrastructure

- Alerts for preventative maintenance

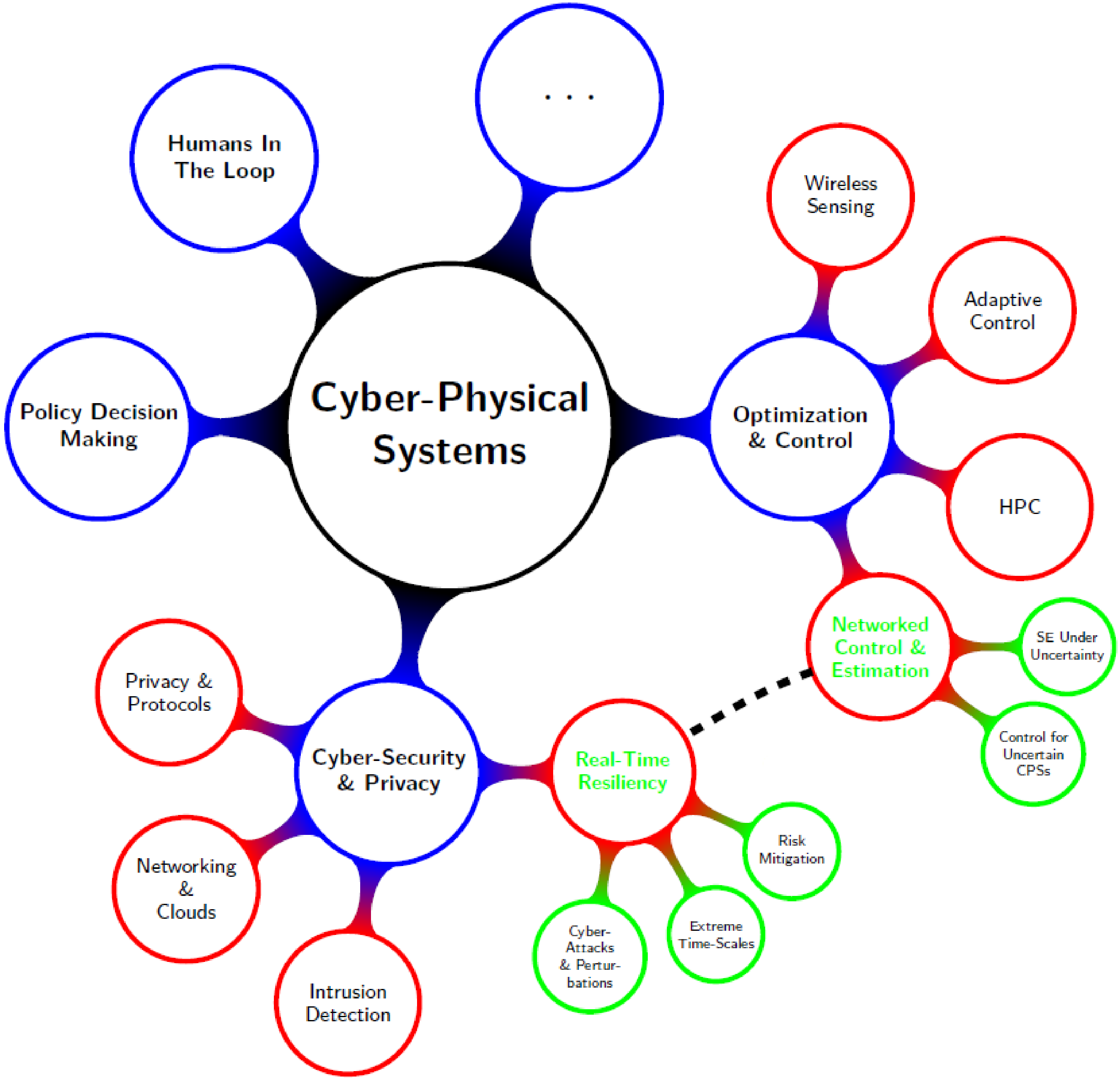
CPS Elements

Electrical Parts

Mechanical Parts

Business Aspects

CYBER Part



CPS Challenges

Integration of different components

- CPS include many components to work together smoothly
- Large scale heterogenous environment – hard to predict

Communication requirements

- Cyber domain needs new protocols that would fulfill time critical requirements

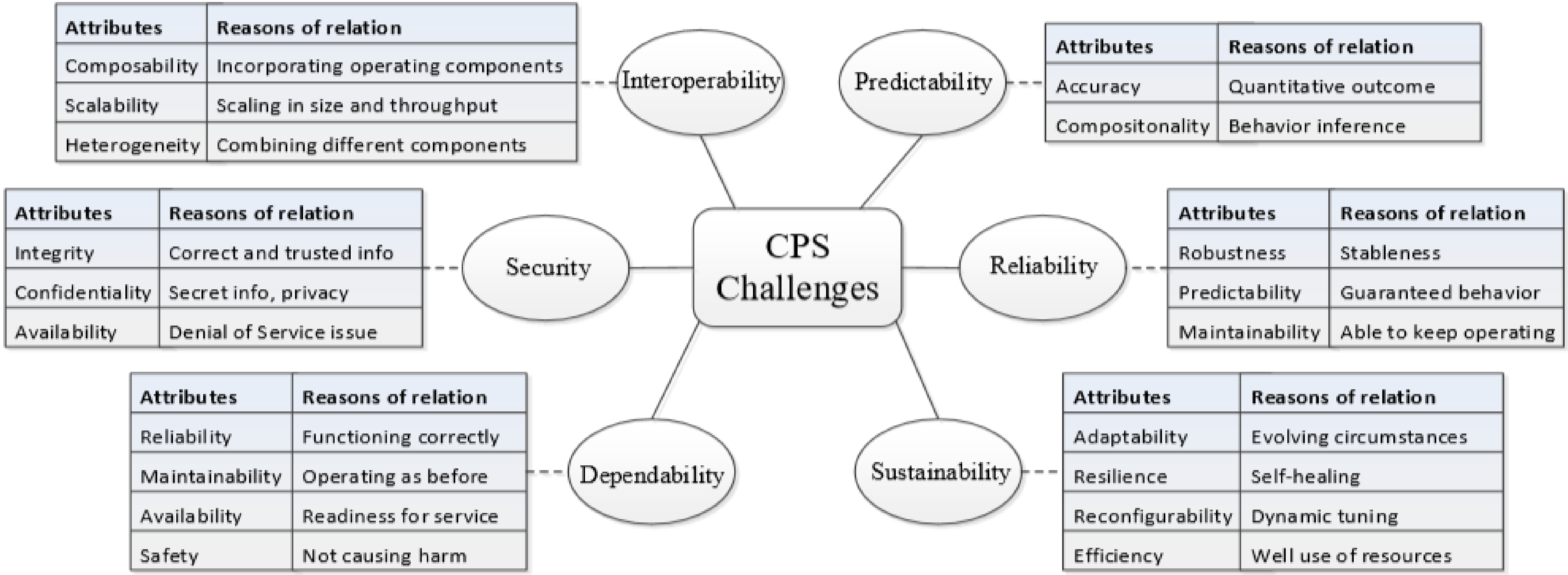
Software validation

- Specific software design for each CPS systems

Societal concerns

- Will people trust anyway?

CPS Challenges



Attributes	Reasons of relation
Composability	Incorporating operating components
Scalability	Scaling in size and throughput
Heterogeneity	Combining different components

Attributes	Reasons of relation
Accuracy	Quantitative outcome
Compositonality	Behavior inference

Attributes	Reasons of relation
Integrity	Correct and trusted info
Confidentiality	Secret info, privacy
Availability	Denial of Service issue

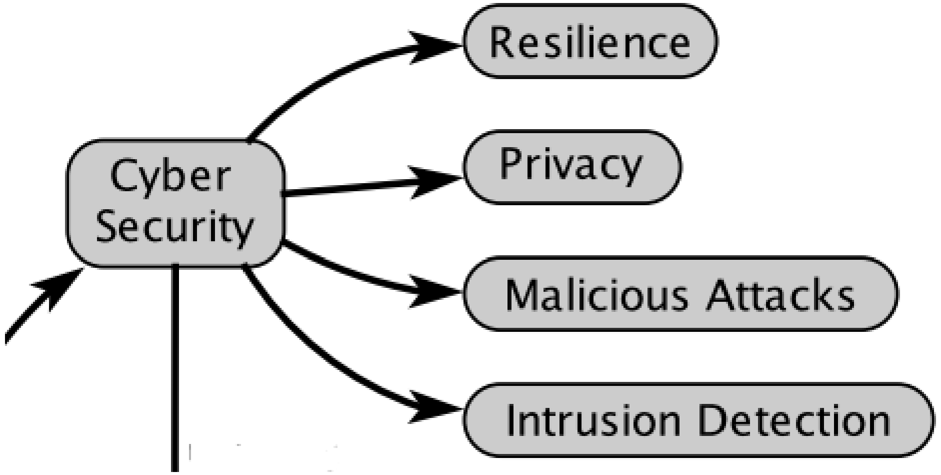
Attributes	Reasons of relation
Robustness	Stableness
Predictability	Guaranteed behavior
Maintainability	Able to keep operating

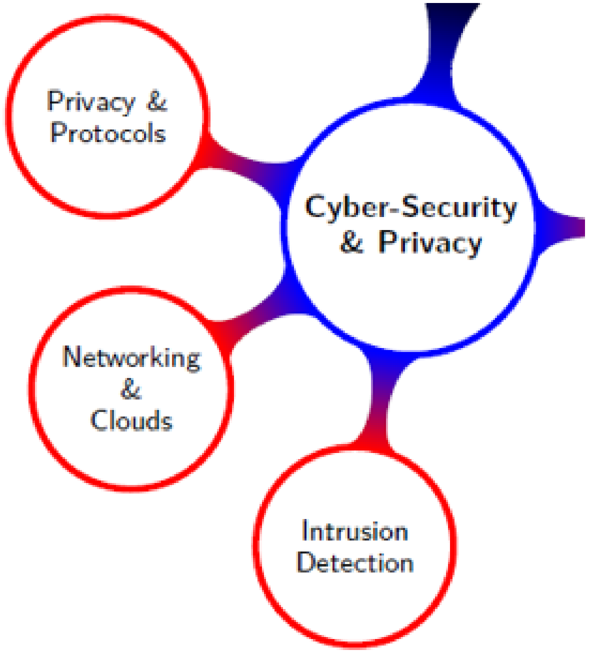
Attributes	Reasons of relation
Reliability	Functioning correctly
Maintainability	Operating as before
Availability	Readiness for service
Safety	Not causing harm

Attributes	Reasons of relation
Adaptability	Evolving circumstances
Resilience	Self-healing
Reconfigurability	Dynamic tuning
Efficiency	Well use of resources

Our Focus

Focus of this Course:





CPS Security Challenges

Security

- Authentication, authorization, encryption, etc.

Resiliency

- If one part fails, will system collapse?
- Is failure due to (cyber) attack or physical conditions?

Privacy

- Who will see which kind of personal data?

CPS Distinguishing Characteristics: Security Aspect

Traditional (IT) security:

Access restriction and control can be applied without affecting the system services.

Confidentiality is ranked the first security objective for IT systems

Traditional security techniques individually focus on addressing security for system components

CPS security:

Could affect or delay the real-time response of the physical parts of CPS

Availability comes first for CPS, then integrity, confidentiality and authenticity.

The interactions among these components

Why CPS Security matters?

For instance: A successful cyber attack on energy CPS can;

- delay, block, or alter the intended process, that is, alter the amount of energy produced at an electric generation facility
- delay, block, or alter information related to a process, thereby preventing a bulk energy provider from obtaining production metrics that are used in energy trading or other business operations