



---

**KENNESAW STATE**  
UNIVERSITY






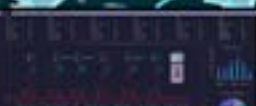


## **Module 2: Physical Platforms and Elements**

**Dr. Maria Valero**

# Agenda

- Physical Systems Description and Classification
- Layers in Physical Systems
- CPS Layers Components
- CPS Security Threats
- CPS Security Countermeasures

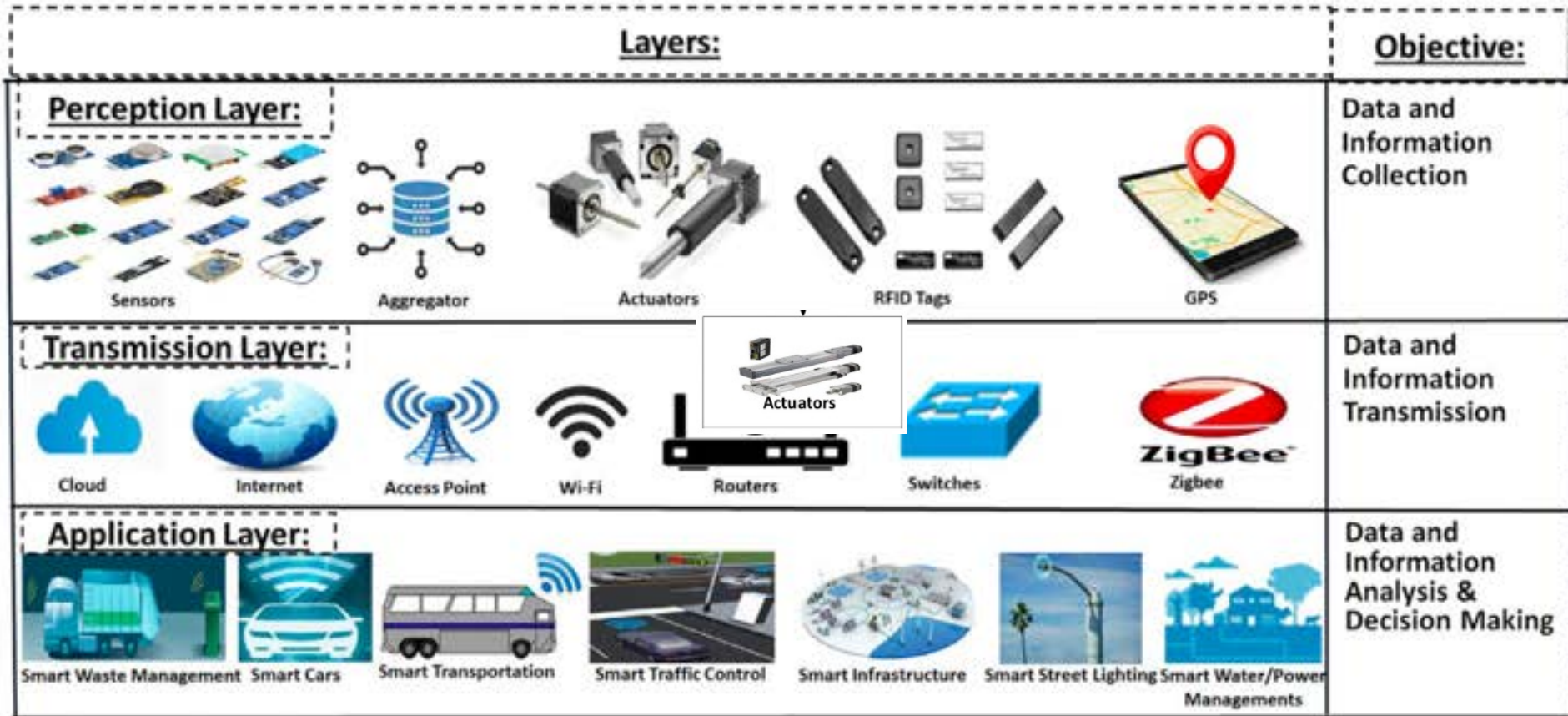
# Physical Systems Classification

Naming	Classification	Description
 <b>Smart House</b>	<b>Industrial-Consumer IoT</b>	<ul style="list-style-type: none"> <li>• <b>Control Smart Devices</b></li> <li>• <b>Homeowner Security &amp; Comfort</b></li> </ul>
 <b>Oil Refinery</b>	<b>Industrial-Transportation IoT</b>	<ul style="list-style-type: none"> <li>• <b>Naphta, Gasoline, Diesel</b></li> <li>• <b>Asphalt, Petroleum, Fuel, Oil</b></li> </ul>
 <b>Smart Grid</b>	<b>Industrial IoT</b>	<ul style="list-style-type: none"> <li>• <b>Smart Efficient Energy</b></li> <li>• <b>Energy Control &amp; Management</b></li> </ul>
 <b>Water Treatment</b>	<b>Industrial-Consumer IoT</b>	<ul style="list-style-type: none"> <li>• <b>Improved Water Quality</b></li> <li>• <b>Overcome Contamination &amp; Undesirable Components</b></li> </ul>
 <b>Medical Devices</b>	<b>Medical-Wearable IoT</b>	<ul style="list-style-type: none"> <li>• <b>Improved Patients Life</b></li> <li>• <b>Enhanced Medical Treatment</b></li> <li>• <b>Remote Patient Monitoring</b></li> </ul>
 <b>SCADA</b>	<b>Industrial IoT</b>	<ul style="list-style-type: none"> <li>• <b>Control &amp; Monitor Telecoms.</b></li> <li>• <b>Control &amp; Monitor Industries</b></li> </ul>
 <b>Smart Cars</b>	<b>Industrial-Transportation IoT</b>	<ul style="list-style-type: none"> <li>• <b>Echo Friendly</b></li> <li>• <b>Enhanced Driver Experience</b></li> <li>• <b>Advanced Safety Features</b></li> </ul>
 <b>Supply Chains</b>	<b>Industrial-Transportation IoT</b>	<ul style="list-style-type: none"> <li>• <b>Real-Time Delivery Source/Destination</b></li> <li>• <b>Less Delays &amp; Echo Friendly</b></li> </ul>



Physical Systems Layers

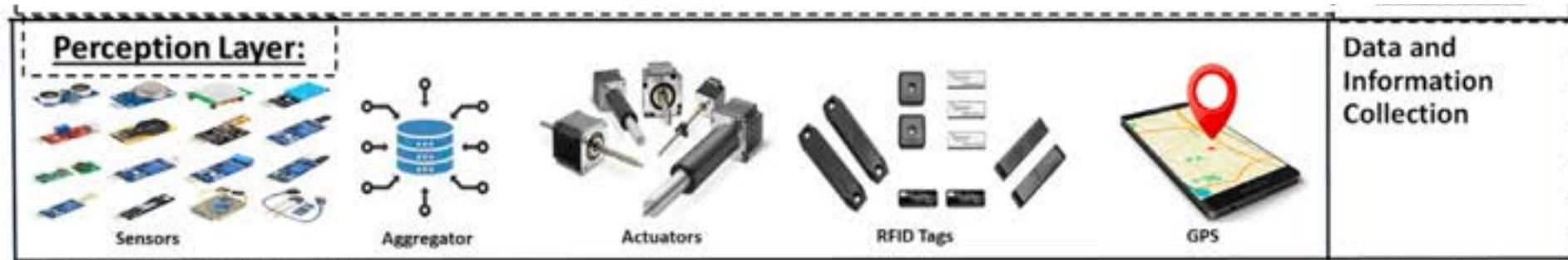
# CPS Layers Overview



- Image from Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201.

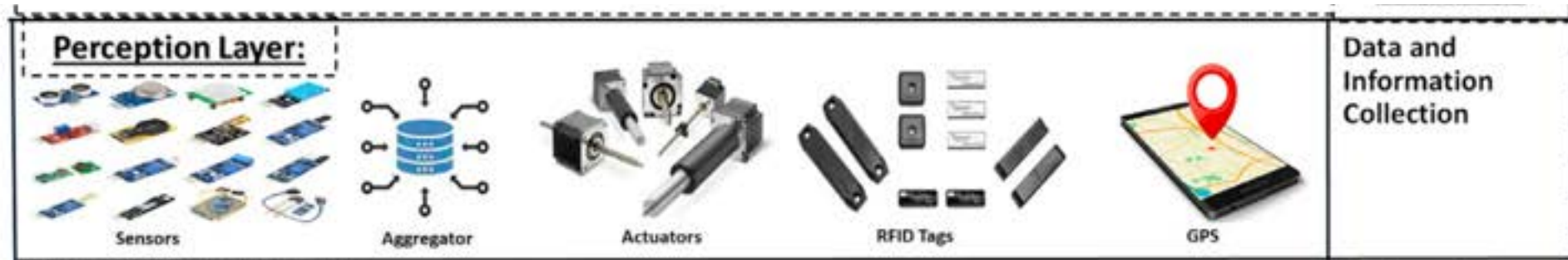
# Perception Layer

- Also known as "Sensing Layer"
- It includes equipment such as sensors, actuators, aggregators, Radio-Frequency Identification (RFID) tags, Global Positioning Systems (GPS) along with various other devices
- These devices collect real-time data in order to monitor, track and interpret the physical world



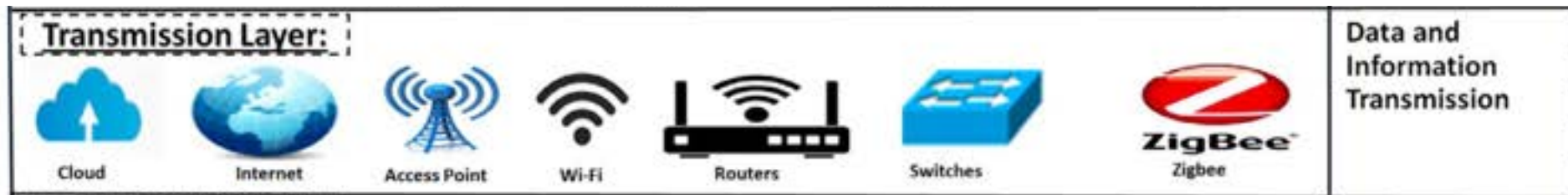
# Perception Layer - Examples

- Examples of such collected data include electrical consumption, heat, location, chemistry, and biology, in addition to sound and light signals, depending on the sensors' type.
- These sensors generate real-time data within wide and local network domains, before being aggregated and analyzed by the application layer.



# Transmission Layer

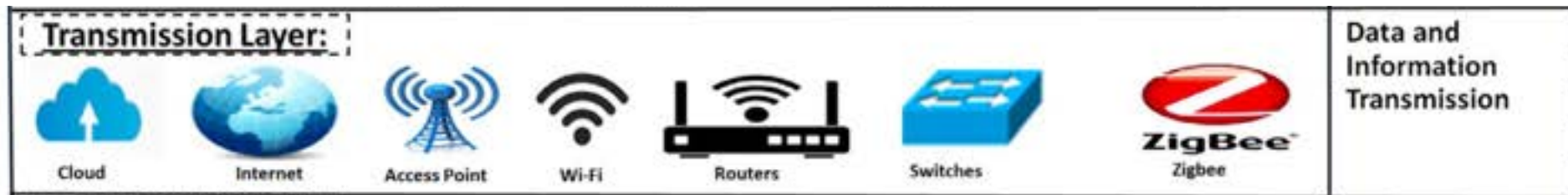
- Also known as "Transport Layer" or "Network Layer"
- It interchanges and processes data between the perception and application layers
- It can use Local Area Networks (LANs) and communication protocols including Bluetooth, 4G and 5G, InfraRed (IR) and ZigBee, Wi-Fi, Long Term Evolution (LTE), along with other technologies





# Transmission Layer (2)

- This layer also ensures data routing and transmission using cloud computing platforms, routing devices, switching and internet Gateways, firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)



# Application Layer

- It processes the received information from the data transmission layer and issues commands, which are executed by the physical units including sensors and actuators
- It implements complex decision-making algorithms based on the aggregated data
- This layer receives and processes information from the perception layer before determining the rightly invoked automated actions

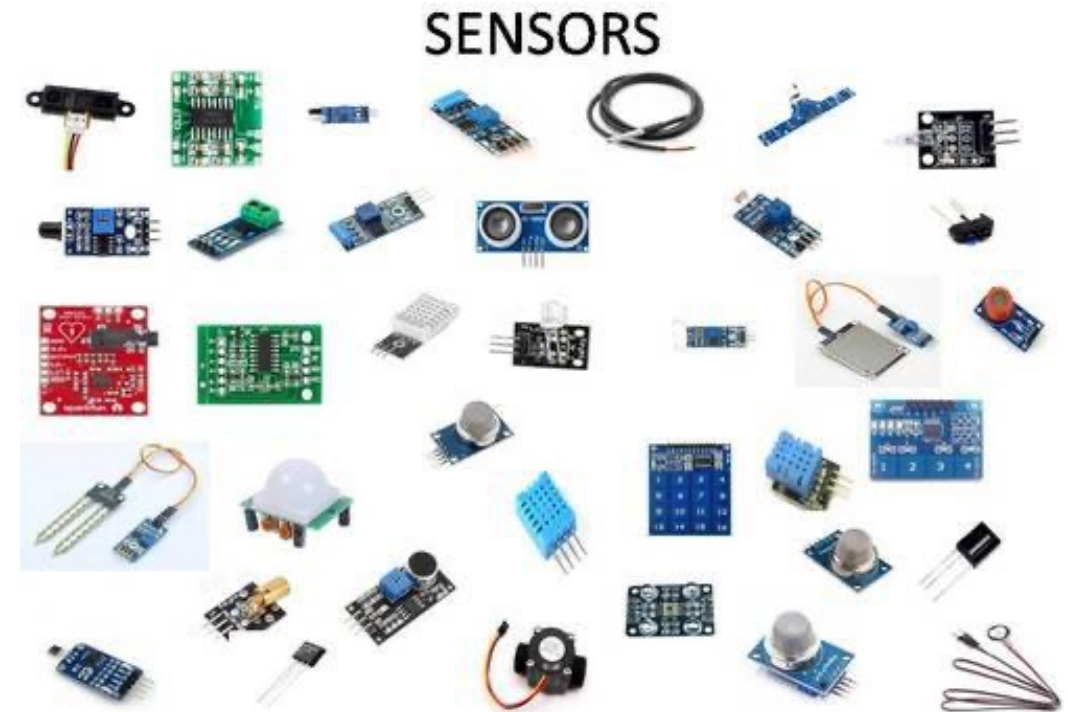


# CPS Layers - Components



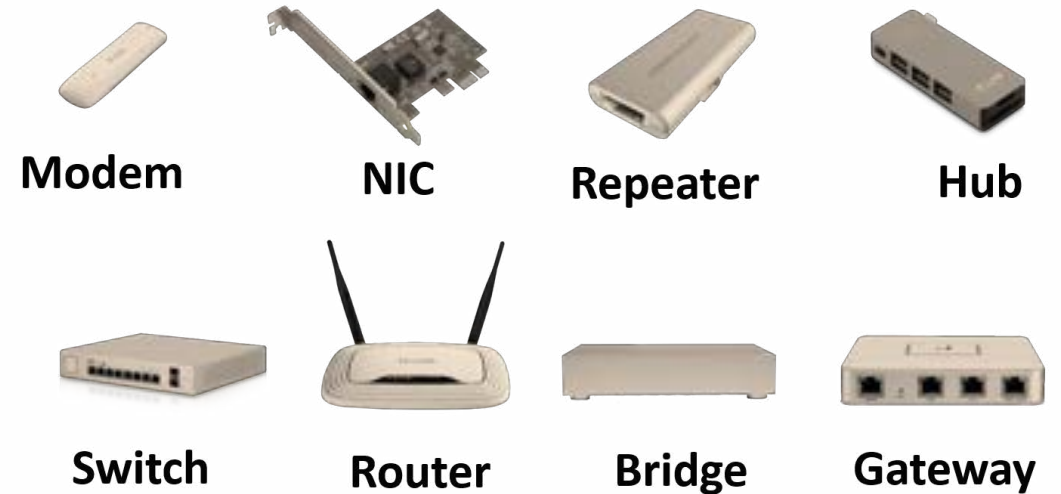
# Sensing Components (1)

- Located in the Perception Layer and consists of sensors that collect data/information.
- Types of Sensing Components
  - SENSORS: Collect and record real-world data following a correlation process named "calibration", to assess the correctness of the collected data.



# Sensing Components (2)

- Types of Sensing Components
  - Aggregators : Are primary located at the transmission layer (i.e., routers, switches, gateways) to process the received data/information from the sensors, before issuing the corresponding decision(s). The aggregation is based on the collected information about the specific target, where data is gathered and summarized following a statistical analysis.
    - OLAP (Online Analytical Processing) is a prime data aggregation type



# Sensing Components (3)

- Types of Sensing Components
  - Actuators : Are primary located at the application to make the information visible to the surrounding environment based on the decisions made by the aggregators. Actuators process electrical signals as input and generate physical actions as output



# Controlling Components (1)

- Those are used to control signals and they play a key role in monitoring and management to achieve higher levels of accuracy and protection against attacks.
- Types of Controlling Components
  - Programmable Logic Controllers (PLC): Are considered an industrial digital computers that control the manufacturing processes such as robotics devices performance and/or fault diagnosis processing;



# Controlling Components (2)

- Types of Controlling Components
  - Distributed Control Systems (DCS):  
Are computerized control systems that allow the autonomous controllers' distribution throughout the system using a central operator supervisory control. As a result of the remote monitoring and supervision process, the DCS's reliability is increased, whilst its cost is reduced. In some cases, DCS can be similar to Supervisory Control and Data Acquisition (SCADA) systems





# Controlling Components (3)


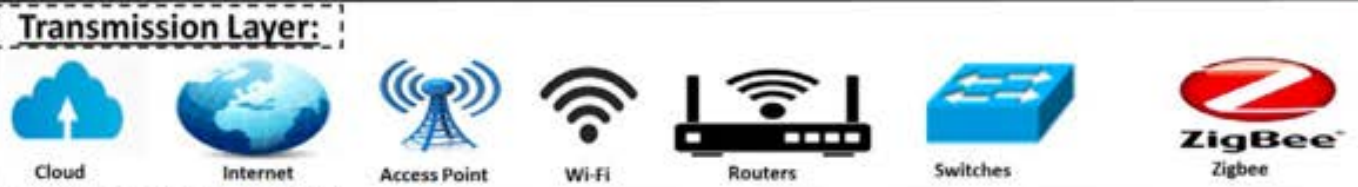

- Types of Controlling Components
  - Remote Terminal Units (RTU): are electronic devices controlled by a microprocessor such as the Master Terminal Unit (MTU). Unlike PLC, they do not support any control loop nor control algorithm(s). This, making them more suitable for wireless communications over wider geographical telemetry areas. RTU main task is to interface SCADA to physical object(s) using a supervisory messaging system that controls these objects.



A glowing green padlock is centered on a dark blue background with a complex circuit board pattern. The padlock has a bright, shimmering green glow. The circuit board pattern consists of numerous thin, light blue lines and dots, creating a dense, intricate network. The overall lighting is dark, with the green padlock and the blue circuit lines providing the primary visual elements.

# CPS Security Threats

# CPS Threat Attacks and Targets

Layers:		Objective:	Threat/Attack:	Target:
<b>Perception Layer:</b> 		Data and Information Collection	<ul style="list-style-type: none"> <li>Eavesdropping</li> <li>Port Scan</li> <li>Passive Replay</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Privacy</li> <li>Authentication</li> </ul>
<b>Transmission Layer:</b> 		Data and Information Transmission	<ul style="list-style-type: none"> <li>Man-in-the-Middle</li> <li>Meet-in-the-Middle</li> <li>DoS/ D-DoS</li> <li>Repudiation</li> <li>Replay –</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Authentication</li> </ul>
<b>Application Layer:</b> 		Data and Information Analysis & Decision Making	<ul style="list-style-type: none"> <li>Malicious Code Injection</li> <li>Botnets - malware</li> <li>Trojans</li> <li>Worms</li> <li>Buffer Overflow</li> </ul>	<ul style="list-style-type: none"> <li>Privacy</li> <li>Security</li> <li>Safety</li> <li>Authentication</li> </ul>

- Image from Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201.

# CPS Cyber Threats (1)

- CPS Systems are prone to:

Attack	Description
Wireless Exploitations	Attackers exploit wireless capabilities to gain remote access or control over the system
Jamming	Attackers change the device's state and the expected operations to cause damage by launching waves of de-authentication or DoS
Reconnaissance	Attackers violate data confidentiality (specially in industrial control systems and nation agencies)
Remote Access	Attackers gain remote access to CPS infrastructure, for example, causing disturbances, financial losses, blackouts, etc. Havex Trojans are among the most dangerous malware against ICSs.

# CPS Cyber Threats (2)

- CPS Systems are prone to:

Attack	Description
Disclosure of Information	Attackers can disclose any private/personal information through the interception of communication traffic.
Unauthorized Access	Attackers gain an unauthorized access through either a logical or physical network and retrieve important data
Interception	Attackers intercept private conversations through the exploitation of already existing or new vulnerability
GPS Exploitation	Attackers track a device or even a car by exploiting GPS navigation systems, resulting in a location privacy violation
Information Gathering	Attackers gather files and audit logs on any given device in order to sell this huge amount of personal information for marketing and commercial purposes

# CPS Physical Threats (1)

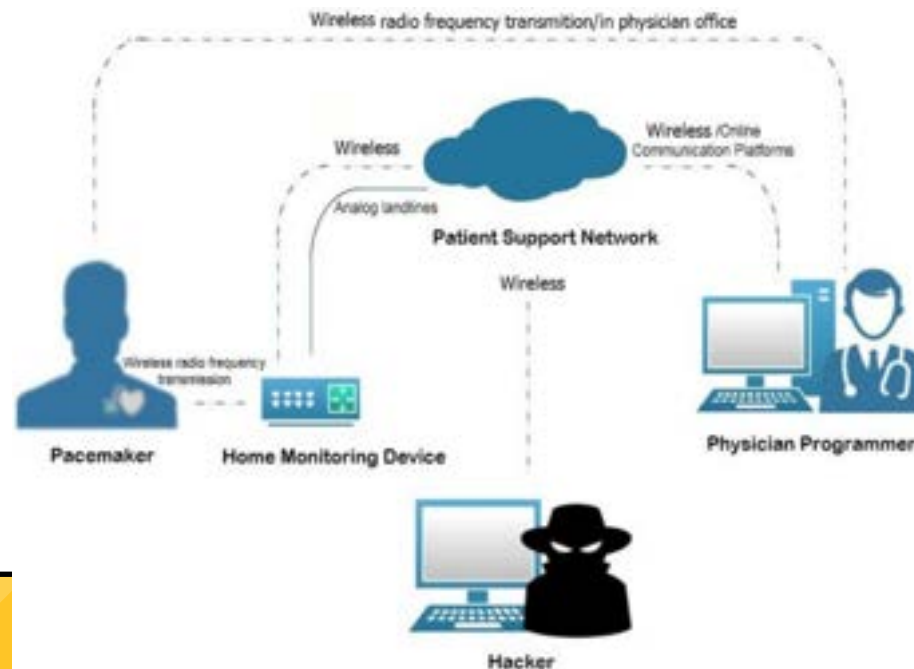
- CPS Systems are prone to:

Attack	Description
Spoofing	It consist of masquerading the identity of a trusted entity to spoof sensors, for example, by sensing misleading and/or false information to the control center
Sabotage	It consist of intercepting the legal communication traffic and redirecting it to malicious third party or disrupting the communication process. For example, attackers can sabotage physically exposed CPS components across the power system, to cause disruption or DoS or blackout
Service Disruption or Denial	Attackers are capable of physically tampering with any device to disrupt a service or to change the configuration. Very critical for medical application

# CPS Physical Threats (2)

- CPS Systems are prone to:

Attack	Description
Tracking	Since devices are physically exposed, an attacker can gain access to a given device, and/or even attach a malicious device or track the legal ones.



# CPS Threat Countermeasures

