IoT, Cyber-Physical Systems and Security

Dr Ayman El Hajjar

The lecture maps to the following CyBOK Knowledge Areas:

Full Coverage:

- Infrastructure Security $\rightarrow$ Cyber-Physical Systems Security

Partly Covered:

- Infrastructure Security $\rightarrow$ Network Security
- Systems Security $\rightarrow$ Authentication, Authorisation & Accountability
- Human, Organisational & Regulatory Aspects $\rightarrow$ Risk Management & Governance

Outline

Introduction to IoT and CPS

What is IoT?

The **Internet of Things (IoT)** is a network of physical devices connected to the Internet that can collect, exchange, and process data.

IoT technologies are used in a wide range of environments to support monitoring, automation, and data-driven decision making.

IoT Applications

IoT technologies are used across many sectors to monitor physical environments, exchange data, and support automated decision making. Examples of common application domains include:

- Consumer IoT (smart homes, wearables)
- Healthcare IoT (medical monitoring, connected devices)
- Industrial IoT (manufacturing, process control)
- Transportation (connected and autonomous vehicles)
- Smart Cities (traffic, lighting, public services)
- Environmental and Agricultural Monitoring

What is a Cyber-Physical System?

A **Cyber-Physical System (CPS)** integrates computation, communication, and physical processes to monitor and interact with the physical world.

- Sensors collect information from the physical environment.
- Networks transfer data between system components.
- Software analyses data and makes decisions.
- Actuators perform actions that affect the physical world.

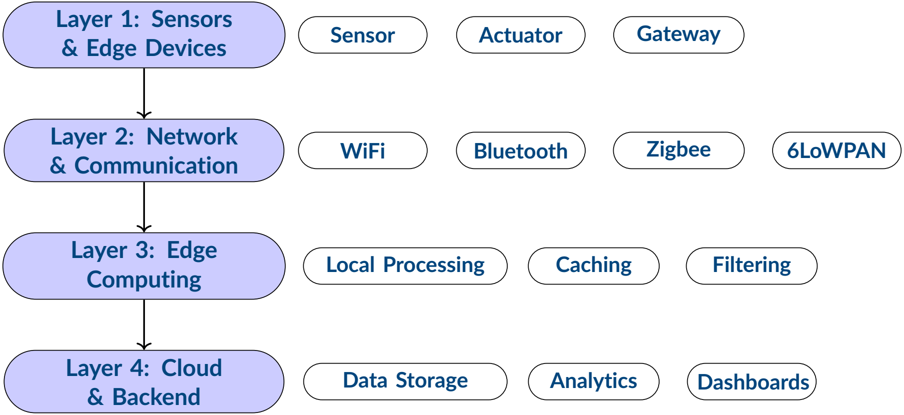
CPS Application Domains

Cyber-Physical Systems are used in environments where software interacts with and influences physical processes. Examples of common application domains include:

- Industrial Control Systems (manufacturing, process control)
- Healthcare Systems (medical devices, patient monitoring)
- Transportation Systems (connected and autonomous vehicles)
- Smart Grids (energy generation and distribution)
- Smart Buildings (HVAC, lighting, access control)
- Critical Infrastructure (water treatment, rail, power systems)

IoT and CPS Architecture

IoT Reference Architecture



Data flows up the stack; control flows down. Each layer has different **security requirements**.

IoT Communication Technologies

- **Short-Range and Low-Power Wireless**
  - **Bluetooth / BLE:** Wearables and personal devices
  - **Zigbee:** Home automation and mesh networks
  - **6LoWPAN:** IPv6 over constrained low-power wireless networks
  - **NFC:** Contactless communication

- **Medium-Range Wireless**
  - **WiFi:** Home and enterprise networks

- **Long-Range Wireless**
  - **Cellular (LTE/5G):** Mobile and remote deployments
  - **LoRaWAN:** Low-power wide-area networks

IoT Messaging Protocols

Messaging protocols define how IoT data and commands are exchanged above the underlying network technology.

- **MQTT:** Lightweight publish-subscribe messaging commonly used by sensors, gateways and dashboards
- **CoAP:** Lightweight request-response protocol designed for constrained devices
- **HTTP/REST:** Common web-based communication model, but usually heavier than MQTT or CoAP

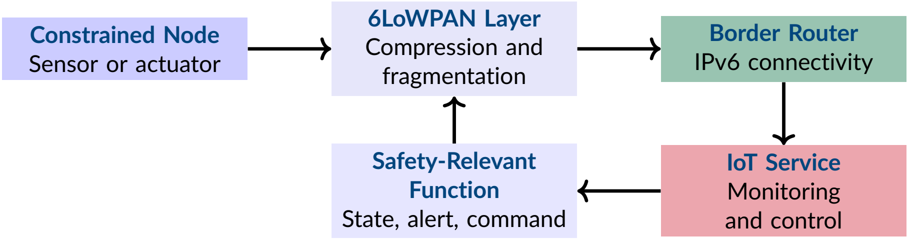
6LoWPAN in Constrained IoT Systems

6LoWPAN

Enables **IPv6 communication** over constrained low-power wireless networks, such as IEEE 802.15.4.

- **Purpose:** Connect constrained sensors and actuators to IP-based networks
- **Constraint:** Devices often have limited power, memory, processing and frame size
- **Adaptation Layer:** Supports header compression, fragmentation and reassembly
- **Border Router:** Connects the low-power wireless network to wider IPv6 networks
- **Safety-Relevant Use:** May carry readings, commands, alerts or device state

6LoWPAN Architecture



6LoWPAN brings **IP networking** into constrained wireless systems that may influence physical behaviour.

Cyber-Physical System (CPS) Architecture

Feedback loop: cyber decisions influence the physical process, and physical changes generate new data.

Key Characteristics of Cyber-Physical Systems

- CPS combine cyber components with physical processes.
- Sensors continuously monitor the physical environment.
- Decisions made by software can affect the physical world.
- Failures may have safety, operational, or financial consequences.

CPS Components

- **Physical Process:** The real-world system being monitored or controlled.
- **Sensors:** Collect information from the physical environment.
- **Communication Network:** Transfers data between system components.
- **Controllers:** Analyse data and make decisions.
- **Actuators:** Perform actions that influence the physical process.
- **Feedback Loop:** Continuous interaction between cyber and physical components.

Security Foundations

Security Objectives in IoT and CPS

- **Confidentiality**
  - Protecting sensitive information from unauthorised disclosure
- **Integrity**
  - Ensuring data and system behaviour remain trustworthy
- **Availability**
  - Maintaining access to devices, services, and communications
- **Authenticity**
  - Verifying the identity of devices and users
- **Safety**
  - Preventing security failures from causing physical harm

IoT Security Challenges

Why is IoT security different from traditional IT?

- **Resource Constraints**
  - Limited computing power, memory, and battery life
- **Diversity**
  - Large variety of devices, vendors, and technologies
- **Lifecycle**
  - Long deployment periods with infrequent updates
- **Connectivity**
  - Continuous communication over wired and wireless networks
- **Physical Exposure**
  - Devices are often deployed in accessible environments
- **Safety Impact**
  - Security failures may affect physical processes and safety

Common Threats to IoT and CPS

What threats can affect connected devices and physical processes?

- **Eavesdropping**
  - Intercepting communications to obtain sensitive information
- **Data Manipulation**
  - Modifying sensor readings or control commands
- **Device Impersonation**
  - Spoofing a trusted device or service
- **Denial of Service**
  - Disrupting communications or system availability
- **Physical Tampering**
  - Gaining physical access to devices, sensors, or actuators

IoT Attack Vectors

How can IoT systems be attacked?

- **Device Layer**
  - Physical access, firmware extraction, key theft
- **Network Layer**
  - Interception, disruption, or manipulation of communications
- **Cloud and Applications**
  - Compromise of services, databases, or user accounts
- **Supply Chain**
  - Vulnerabilities introduced during development or updates
- **Ecosystem**
  - Compromise of gateways or interconnected devices

Security Controls in IoT and CPS

How can we protect IoT devices and cyber-physical systems?

- **Authentication**
  - Verify the identity of users, devices, and services
- **Access Control**
  - Restrict access to authorised entities
- **Encryption**
  - Protect data during storage and transmission
- **Secure Updates**
  - Patch vulnerabilities throughout the device lifecycle
- **Monitoring**
  - Detect abnormal behaviour and potential attacks

Real-World Examples

Real-World Example: Healthcare

Security failures can become patient safety issues

Security Incident	System Behaviour	Safety Impact
Compromise of a connected medical device	Incorrect data or unauthorised commands	Delayed, incorrect, or unsafe treatment

Example

Researchers have demonstrated attacks against connected insulin pumps and pacemakers.

Real-World Example: Critical Infrastructure

Cyber attacks can affect physical infrastructure

Security Incident	System Behaviour	Safety Impact
Compromise of an industrial control system	Disrupted or manipulated operations	Service outages, equipment damage, or injury

Example

Recent incidents have targeted pipelines, power systems, and water treatment facilities.

Summary

- **Internet of Things (IoT)** connects physical devices, sensors, and services through communication networks
- **Cyber-Physical Systems (CPS)** integrate computation, communication, and physical processes
- **IoT and CPS architectures** consist of multiple layers from devices to cloud services
- **Communication technologies and protocols** enable data exchange between system components
- **Security objectives** include confidentiality, integrity, availability, authentication, and privacy
- **IoT systems face unique challenges** due to resource constraints, diversity, connectivity, and lifecycle issues
- **Security incidents** can influence system behaviour and lead to real-world safety consequences

Key References

- NCSC. *Device security principles for manufacturers*. **[Link]**
- NIST. (2019). *Cyber-Physical Systems and Internet of Things*. NIST SP 1900-202. **[Link]**
- ENISA. (2020). *Guidelines for Securing the Internet of Things*. **[Link]**
- OWASP. Internet of Things Project (Top 10). **[Link]**