CPS IMP QUES

2M

UNIT 1

1. DEFINE CYBER PHYSICAL SYSTEM

- CPS integrates physical devices with computer systems.
- It uses sensors, controllers, and networks.
- Real-time data is collected and processed.
- Examples: Smart grid, autonomous vehicles

2. DIFFERENTIATE AR AND VR

Augmented Reality (AR)	**Virtual Reality (VR)**
Adds digital elements to the real world	Creates a fully virtual environment
Real world is still visible	Real world is completely blocked
Uses phones or AR glasses	Uses VR headsets
Example: Snapchat filters	Example: VR games like Beat Saber

3. WHAT IS GLOBALIZATION

- Globalization connects countries through trade and communication.
- It allows free movement of goods, services, and ideas.
- Businesses can operate in multiple countries.
- It promotes cultural exchange and global cooperation.

UNIT 2

1. DEFINE EMBEDDED SYSTEMS

- A system built into a device to perform a specific task.
- It combines hardware and software.
- Mostly has limited computing resources.
- Examples: Microwave oven, digital watch.

2. WHAT IS THE REAL TIME SCHEDULING ISSUES IN CPS

- Tasks must complete within strict deadlines.
- Delay in one task can affect the entire system.
- Multiple tasks compete for limited resources.
- Predictability and reliability are difficult to maintain.

3. WHAT IS DISCRETE EVENT SCHEDULING

- Events are scheduled only when specific conditions occur.
- It saves resources by not running continuously.
- Common in simulations and manufacturing.
- Example: Scheduling machines in a factory when needed.

UNIT 3

1. WHAT IS MEANT BY SIGNAL PROCESSING.

- It deals with analysis and modification of signals.
- Signals can be sound, image, or sensor data.
- Helps remove noise and improve quality.
- Used in mobile phones, medical devices, etc.

2. DEFINE CONFIGURATION MANAGEMENT

- It manages changes in system software and hardware.
- Ensures consistency and reliability.
- Tracks versions and updates in systems.
- Important for maintaining large systems.

3. DEFINE ROUTING

- Routing finds the best path for data in a network.
- It ensures data reaches the correct destination.
- Routers and algorithms handle the routing.
- Used in internet, GPS, and wireless networks.

UNIT 4

1. HOW SECURITY IS PROVIDED TO CPS

- Using encryption to protect data.
- Authentication to verify user access.
- Firewalls to block unauthorized access.
- Intrusion detection systems to monitor threats.

2. GIVE THE PRIVACY ISSUES IN VEHICULAR DEVICES AND SMART METERING

- Location data from vehicles can track user movement.
- Driving behavior may reveal personal habits.
- Smart meters show when people are home.
- Risk of data misuse if not protected properly.

3. WRITE ABOUT DIGITAL CERTIFICATES

- A digital certificate is like an online ID card.
- It confirms the identity of a website or user.
- It uses encryption to protect information.
- Issued by trusted authorities (CAs).

12M

UNIT 1

1. EXPLAIN THE INDUSTRY 4.0 IN DETAIL

What is Industry 4.0?

Industry 4.0 refers to the fourth industrial revolution, which focuses on smart automation, digitalization, and data exchange in manufacturing and other industrial processes. It goes beyond traditional industry to include smart cities, healthcare, transportation, and more.

Evolution of Industrial Revolutions

Revolution	Key Features
1st	Mechanization using steam and water power
2nd	Mass production with electricity and assembly lines
3rd	Automation using electronics and IT systems
4th (Current)	Integration of cyber-physical systems, IoT, AI, cloud computing

Key Technologies in Industry 4.0

Internet of Things (IoT):
Connects physical devices to the internet for data sharing and monitoring.

Industrial IoT (IIoT):
IoT applied specifically in industrial sectors for smart manufacturing.

Cyber-Physical Systems (CPS):
Physical machines integrated with computing and communication systems.

Smart Manufacturing & Smart Factories:
Factories that use automation and data to improve processes and efficiency.

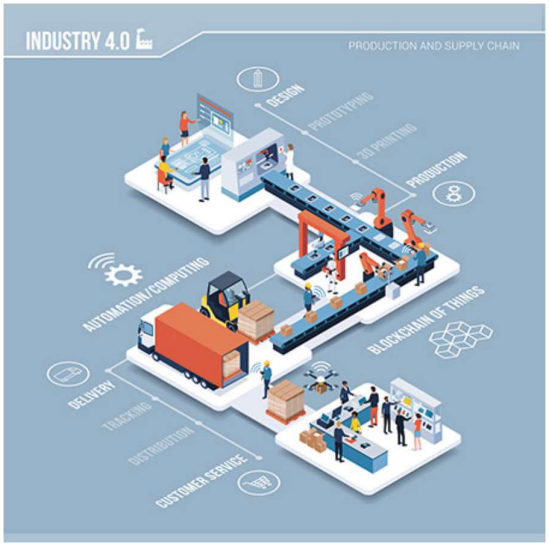
Cloud Computing:
Storing and processing data over the internet for easy access and scalability.

Cognitive Computing & Artificial Intelligence (AI):
Machines learn and make decisions like humans, improving automation and problem-solving.

Digital Twin Technology:
Virtual models of physical systems to simulate, test, and optimize before real-world implementation.

How Industry 4.0 Works

- Machines are equipped with wireless connectivity, sensors, and AI.
- They monitor, analyse, and communicate in real time.
- 5G networks improve response time and allow real-time interaction between devices.
- Digital twins allow virtual testing of products before actual manufacturing.
- Machines can make autonomous decisions and work collaboratively without constant human input.



Core Principles of Industry 4.0

Interconnectivity:
Devices, systems, and people communicate over the IoT.

Information Transparency:
Systems collect real-time data for better decision-making.

Technical Assistance:
AI supports humans by analysing data and helping in complex decisions.

Decentralized Decisions:
Machines make decisions locally without needing central control.

Benefits of Industry 4.0

- Increased productivity
- Better quality control
- Real-time monitoring and decision-making
- Reduced downtime
- Cost-effective production

Example of Industry 4.0 in Use

- In automotive manufacturing, robots work alongside humans using real-time data.
- Offline programming and adaptive control in arc welding show how simulation and production are connected.
- Smart factories in various countries already use these technologies for efficient production.

Challenges in Implementing Industry 4.0

- Multidisciplinary Complexity:
- Lack of Unified Design Language:
- Need for Co-Simulation Tools:
- Standardization Issues:

2. A. EXPLAIN THE COLLABORATIVE PLATFORM AND PRODUCT LIFECYCLE MANAGEMENT

Collaborative Platform

A collaborative platform is a virtual workspace where team members can work together on projects by sharing resources, tracking tasks, and communicating efficiently.

Features:

- Centralized workspace: Everything (documents, updates, tasks) is in one place.
- Real-time communication: Teams can chat, comment, and update each other.
- Project management: Helps in tracking progress and managing tasks.
- Document sharing: Upload and edit files like Word, Excel, PDFs, etc.

Main Goals:

- Improve teamwork and communication.
- Make project tracking and updates easier.
- Save time and money for the business.
- Enhance employee productivity and well-being.

Examples of Collaborative Platforms:

- Microsoft Teams
- Slack
- Trello
- Google Workspace
- Asana

Uses in Business:

- Project portfolio management
- Innovation development
- Continuous improvement activities

Product Lifecycle Management (PLM)?

Product Lifecycle Management (PLM) is the process of managing all the data and activities related to a product — from its idea/design to manufacturing, support, and disposal.

Purpose:

To make sure that everyone involved in a product (like designers, engineers, manufacturers, and service teams) has access to the latest product information at every stage.

Where PLM Is Used:

- Aerospace
- Medical devices
- Electronics
- Industrial machinery
- Automotive and consumer products

Core Functions of PLM:

- Stores all product data: Design files, specifications, documents, etc.
- Manages product structure: Bill of Materials (BOM), components, and parts.
- Controls workflows: For approvals, changes, and updates.
- Tracks materials: For environmental safety and compliance.
- Supports collaboration: Among teams like marketing, engineering, and service.

Essential Elements of PLM:

- Electronic file repository
- Version control and secure access
- Metadata for parts and documents
- Workflow and task assignments
- Integration with ERP systems
- Support for electronic signatures
- Change and configuration management

B. EXPLAIN GLOBALIZATION, ITS THREATS AND EMERGING ISSUES

What is Globalization?

- Globalization is the process where countries become more connected through business, technology, information, and culture.
- It allows free flow of goods, services, people, and ideas across countries.
- The world feels more connected and smaller due to faster communication and travel.

Examples:

- Buying products made in other countries (e.g., Apple phones).
- Watching global movies or using apps like Instagram or TikTok.
- Companies like Amazon, Google, or McDonald's operating in many countries.

Threats of Globalization

1. Cybercrime:

- More online systems = more chances for hacking, data theft, and fraud.
- Criminals can attack from anywhere in the world.

2. Loss of Privacy:

- Personal data is shared across countries through websites and apps.
- Can be misused or sold without users knowing.

3. Job Losses in Some Countries:

- Companies may move jobs to countries with cheaper labour (outsourcing).
- This can cause unemployment in developed countries.

4. Economic Dependency:

- If one country stops supplying important goods (like fuel or medicine), others suffer quickly.
- Example: COVID-19 supply chain issues.

Emerging Issues in Globalization

1. Digital Divide:

- Some countries have fast internet and modern tech.
- This creates inequality in access to information and opportunities.

2. Cultural Loss:

- Local languages, traditions, and values may fade away as global culture spreads.

3. Environmental Damage:

- More global trade means more factories, pollution, and waste.
- Climate change becomes a bigger global issue.

4. Security Challenges:

- Terrorism and cyberattacks can spread faster through global networks.
- Harder to track and control crimes across borders.

UNIT 2

1. SUMMARIZE REAL-TIME OPERATING SYSTEM

- An RTOS (Real-Time Operating System) is an operating system specially designed to handle real-time applications where tasks must be completed within specific time constraints.
- It is used in embedded systems that require deterministic (predictable) behavior.

Scheduler in RTOS:

- The scheduler is the core component that controls task execution.
- In an RTOS, the scheduler is designed to provide a predictable and time-bound execution pattern.
- It ensures multitasking, where multiple tasks are managed without missing deadlines.

Why RTOS is Needed in Embedded Systems:

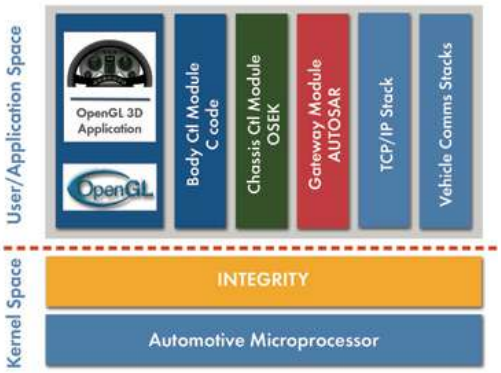
- Embedded systems often control critical hardware (e.g., cars, medical devices, robots).
- These systems must respond to events in real time (within a strict time window).
- RTOS ensures tasks are completed on time and reliably.

Features of RTOS:

- Short Context Switching Latency
- Short Interrupt Latency
- Short Interrupt Dispatch Latency
- Predictable Task Scheduling
- Reliable Inter-process Communication
- Kernel Pre-emption Support
- Task Prioritization
- Real-Time Clocks & Timers
- Minimal Jitter
- Deterministic Execution

Responsibilities of RTOS:

- Task Management and Scheduling
- Interrupt Handling
- Inter-Process Communication
- Task Synchronization
- Memory Management



- Automotive Microprocessor – Hardware platform that runs the automotive system.
- INTEGRITY (RTOS) – Real-Time Operating System that manages tasks and resources securely.
- OpenGL 3D Application – Used for rendering graphics on automotive displays.
- OpenGL – Graphics API used by 3D applications for visual output.
- Body Control Module (C Code) – Manages body-related functions like doors, lights, and wipers.

Types of RTOS:

Type	Description	Example
Hard Real-Time	Missing deadlines is not allowed. Fails if deadline is missed.	Flight control, pacemakers
Soft Real-Time	Occasional deadline misses are acceptable.	Video streaming, data collection
Real Real-Time	Requires ultra-fast, hard real-time response.	Missile guidance, emergency systems
Firm Real-Time	Deadline is important, but late results have no value.	Online transaction processing

AUTOSAR and INTEGRITY RTOS:

- AUTOSAR (AUTomotive Open System ARchitecture) supports INTEGRITY RTOS for automotive applications.
- It enables standardized, secure, and real-time performance for car control systems.

8. Examples of RTOS:

- VxWorks – Used in aerospace systems
- FreeRTOS – Lightweight, open-source RTOS
- INTEGRITY RTOS – Used in automotive and secure embedded systems
- QNX – Real-time OS used in industrial and medical devices
- RTLinux – Real-time version of Linux

9. Applications of RTOS:

- Automotive (ABS, airbags)
- Medical devices (heart monitors)
- Industrial control systems

2. A. EXPLAIN WIRELESS HART AND CAN

WirelessHART

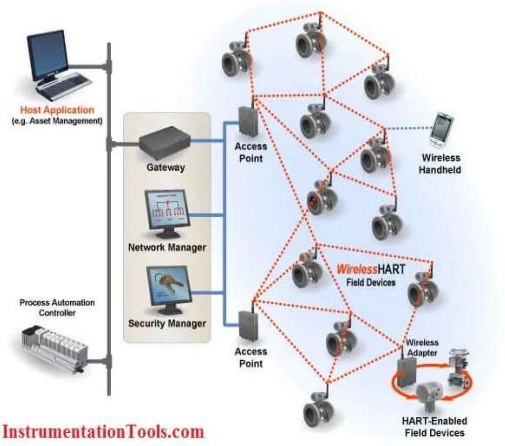
- WirelessHART is a wireless sensor networking protocol for process automation.
- It extends the traditional HART protocol with wireless capability.
- Designed to provide secure, reliable, and cost-effective communication in industrial environments.

Features:

- Mesh Network – Devices form a self-healing mesh to forward messages through multiple paths.
- IEEE 802.15.4 Based – Operates on the 2.4 GHz ISM band, using standard radio technology.
- Time Synchronized – Uses TDMA for latency-controlled communication.
- Channel Hopping – Increases reliability and avoids interference.

Components:

- Wireless Field Devices – Sensors or actuators with built-in WirelessHART or adapters.
- Gateway – Connects the wireless network to host systems (e.g., SCADA, PLC).
- Network Manager – Manages device routes, time slots, and network health.
- Security Manager – Handles encryption keys and device authorization.
- Adapter – Converts wired HART devices into WirelessHART-compatible.
- Repeater – Extends network range; forwards data without sensing.
- Handheld Terminal – Used for configuration, diagnostics, or reading process values.



1. Wireless Field Devices

These are sensors or instruments that measure process variables and communicate wirelessly.

2. Gateway

Acts as a bridge between the wireless field devices and the host system

3. Network Manager

→ Manages the wireless mesh network by scheduling communication, managing routes, and monitoring performance.

Advantages:

- Reduces wiring cost and complexity.
- Reliable due to redundant routing paths.
- Easy to expand by adding new wireless devices.
- Compatible with existing HART tools and commands.

CAN

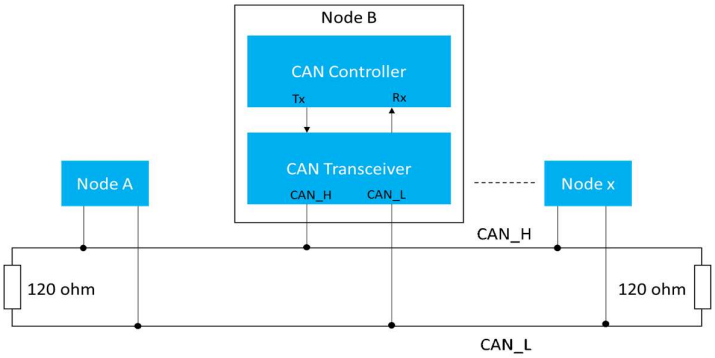
- CAN stands for Controller Area Network, used in automotive and industrial systems.
- It allows microcontrollers and devices (ECUs) to communicate without a host computer.
- Developed to replace complex point-to-point wiring systems.

Features:

- Message-Based Protocol – Communication happens using unique message IDs.
- Differential Signaling (CANH & CANL) – Reduces noise, improves reliability.
- Multi-Master – All nodes can transmit and receive messages.
- Arbitration Mechanism – Resolves data collision when multiple nodes transmit.

Architecture Layers:

- Application Layer – Interfaces with application software.
- Data Link Layer – Manages message formatting, CRC, and acknowledgment.
- Physical Layer – Defines cables, voltage levels, and transceivers.



CAN in Microcontrollers:

- Arduino: Uses CAN Shield with external controller (MCP2515).
- Raspberry Pi: Needs external controller + transceiver via SPI.
- STM32: Has built-in CAN controller; needs only transceiver externally.

Advantages:

- Reliable and robust in noisy automotive environments.
- Reduces wiring and complexity.
- Supports real-time communication.
- Scalable to multiple ECUs and nodes.

B. EXPLAIN ABOUT EMBEDDED AND SOFTWARE TESTING

Embedded Testing

- Embedded testing is used to test the software and hardware together in an embedded system.
- It ensures the entire system works correctly, meets specifications, and is free from defects.
- The goal is to test the functionality, performance, reliability, and safety of the embedded product.
- It is performed during and after development to find and fix issues early.

Purpose of Embedded Testing

- To verify the embedded system works as expected (matches design specs).
- To validate that the system meets user or client needs.
- To reduce development cost by catching bugs early.
- To ensure safety and performance in critical systems (like medical or automotive).
- To support certification processes required by safety standards (like ISO, IEC, etc.).

Types of Embedded Testing

- Unit Testing – Testing individual modules/functions of the software.
- Integration Testing – Testing how software modules interact with each other and with hardware.
- System Testing – Testing the complete embedded system (software + hardware).
- Acceptance Testing – Testing if the system meets client requirements.

Software Testing

- It focuses only on testing the software part of an embedded system.
- It checks that the software is functional, efficient, and reliable.
- It helps identify bugs, security issues, and performance bottlenecks.
- It ensures the software is safe for critical applications (aviation, automotive, railways, etc.).

How Embedded Software Testing is Done

- The software is tested using real hardware, emulators, or simulators.
- Testers provide input values, execute the software, and observe the output and behavior.
- They check if:
- The output is correct
- There are no crashes
- The performance is within acceptable limits

CHALLENGES IN SOFTWARE TESTING

- Hardware Dependency
- Open Source Components
- Software vs. Hardware Defects
- Reproducibility of Defects
- Continuous Software Updates
- Resource Limitations
- Timing and Real-Time Constraints

UNIT 3

1. EXPLAIN IN DETAIL ABOUT WORKING OF SMART SENSORS

A smart sensor is a device that not only senses physical conditions but also has the ability to:

- Process the sensed data,
- Filter and clean it,
- Convert it to a usable format, and
- Communicate it digitally to other systems or devices.

Working Principle of Smart Sensors

A smart sensor works in 5 major steps:

1. Sensing Physical Input

- The sensor detects physical changes from its environment.
- Examples: Temperature, pressure, humidity, acceleration, light, sound, etc.

2. Signal Conditioning

- The raw data (often analog) from the sensor is amplified, filtered, or adjusted.
- For example: Removing unwanted noise, stabilizing the signal, adjusting range.

3. Analog-to-Digital Conversion (ADC)

- The processed analog signal is then converted into digital format.
- This is essential for the microprocessor to understand and process the data.

4. Onboard Data Processing

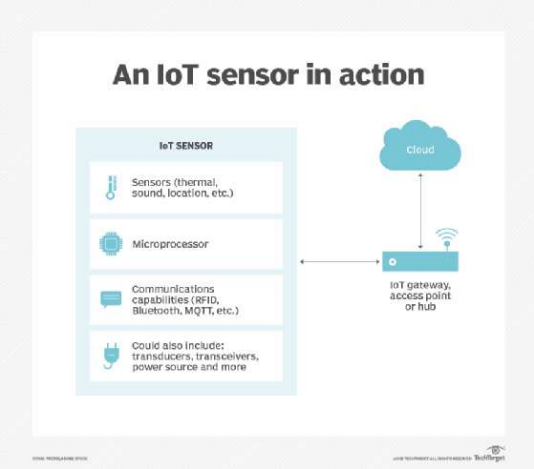
- A built-in microprocessor or microcontroller performs basic computation.
- Tasks include:
- Filtering noise
- Data calibration
- Applying algorithms (like thresholds, averages, etc.)
- Self-diagnosis and error correction

5. Communication to External Systems

- After processing, the smart sensor transmits the digital data to external devices.
- This communication can be via:
- Wired interfaces (e.g., SPI, I2C, UART)
- Wireless protocols (e.g., Wi-Fi, Bluetooth, Zigbee, LoRa)

Components of a Smart Sensor

- Base Sensor – senses physical conditions (e.g., temperature sensor)
- Microprocessor – for computing and logic processing
- Signal Conditioner – filters/amplifies raw signal
- Analog to Digital Converter (ADC) – digitizes the analog signal
- Communication Module – for sending data (Wi-Fi/Bluetooth)
- Software/Algorithms – for data handling, calibration, compensation



IoT Sensor:

- Sensor: Detects data (e.g., heat, sound).
- Microprocessor: Processes the data.
- Communication: Sends data wirelessly.
- Extras: Power and signal helpers.

Gateway/Hub:

- Collects and forwards data to cloud.

Cloud:

- Stores and analyzes data.

Example of Smart Sensor in Use

Industrial Machine Monitoring:

- A vibration sensor monitors a motor.
- If the vibration goes above a certain threshold, the smart sensor processes the signal and alerts the central control system.
- It can even predict a failure before it happens (predictive maintenance).

Key Features of Smart Sensors

- Self-monitoring
- Self-calibration
- Low power usage
- Remote access
- Real-time data reporting
- Wireless or wired communication

Smart Sensors and IoT

Smart sensors are core building blocks of IoT because they:

- Gather data from the physical world,
- Process and interpret it locally,
- Send it to cloud platforms or other systems for analysis or decision-making.

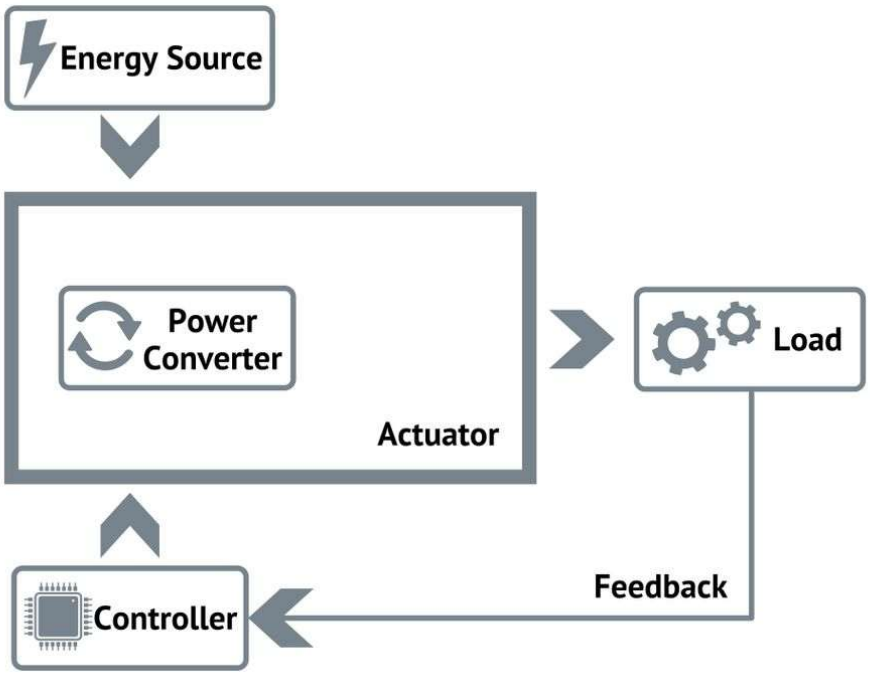
2. ANALYZE THE VARIOUS APPLICATIONS OF ACTUATORS USED IN CYBER PHYSICAL SYSTEM

Actuator

An actuator is a machine component that converts control signals and energy (usually electrical, hydraulic, or pneumatic) into mechanical motion such as pushing, pulling, rotating, or lifting. It allows Cyber-Physical Systems to interact physically with the environment based on computed decisions.

Basic Components of an Actuator in CPS

- Energy Source – Supplies power (electrical, hydraulic, etc.).
- Power Converter – Regulates energy for operation.
- Controller – Generates and manages control signals.
- Load – The mechanical system or component being moved.



Working Principle

An actuator receives a signal from a controller, processes the energy from its power source, and creates motion or force to operate mechanical parts (valves, motors, gates, etc.).

Applications of Actuators in Cyber-Physical Systems

1. Material Handling

- Moves objects via conveyors or robotic arms.
- Automates manufacturing and packaging.

2. Robotics

- Enables precision movements in industrial robots.
- Used for welding, assembling, and inspection tasks.

3. Food & Beverage Manufacturing

- Ensures hygiene with clean, quiet, corrosion-resistant actuators.
- Used in bottle filling, sealing, and packaging.

4. Window Automation

- Automates ventilation in buildings or greenhouses.
- Controlled remotely using smart systems.

5. Agricultural Machinery

- Controls spraying, seeding, or adjusting parts like combine arms.
- Improves accuracy and efficiency in farming operations.

6. Solar Panel Tracking

- Tilts solar panels for optimal sun exposure.
- Enhances energy efficiency through smart adjustment.

7. Cutting Equipment

- Controls blade movement in textile, printing, or carpet industries.
- Offers clean and precise cuts.

8. Valve Operation

- Opens/closes valves in oil, chemical, and food processing plants.
- Allows automated control of liquid or gas flow.

9. Home/Office Automation

- Controls curtains, doors, or adjustable furniture.
- Used for accessibility or comfort in smart homes.

DISADVANTAGES

High cost – some actuators, especially electric or hydraulic ones, can be expensive.

Power consumption – actuators require continuous power to operate, increasing energy use.

Maintenance need – mechanical parts wear out over time and need regular maintenance.

UNIT 4

1. EXPLAIN ELABORATELY ABOUT PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a system of technologies, policies, and procedures used to create, manage, distribute, use, store, and revoke digital certificates. It enables secure communication, authentication, and encryption over untrusted networks (like the internet).

Main Components of PKI

1. Digital Certificates

- Like digital ID cards that verify the identity of users, websites, or devices.
- Bind a public key with an entity (person, system, organization).
- Issued by a Certificate Authority (CA).

2. Certificate Authority (CA)

- A trusted organization that issues, verifies, and manages digital certificates.
- Validates the identity of requesters before issuing a certificate.
- Similar to how a government issues ID cards after verification.

3. Registration Authority (RA)

- Acts as a mediator between the user and CA.
- Verifies user identity and forwards certificate requests to CA.
- Helps manage issuance, renewal, and revocation of certificates.

4. Certificate Database

- Stores all issued, revoked, or expired certificates securely.
- Helps verify certificate history and status.

5. Certificate Store

- Located on devices, stores private keys and certificates.
- Ensures that secure applications can access them for encryption and authentication.

Public Key Cryptography Applications

- Digital Signatures
- Encryption
- Authentication
- Non-repudiation
- Integrity
- Confidentiality
- Key Generation
- Signing & Verification

Symmetric Key Cryptography Applications

- Uses a single shared key for both encryption and decryption.
- Much faster and efficient than public key cryptography.

Suitable for:

- Payment systems (e.g., credit card processing)
- Banking transactions
- Data storage encryption
- Secure messaging apps
- Used when speed and efficiency are critical.

Certificate Revocation List (CRL)

- A list of certificates that have been revoked before expiration.
- Helps browsers or systems know which certificates can no longer be trusted.

Online Certificate Status Protocol (OCSP)

- An online method for checking the real-time status of a certificate.
- Faster and more dynamic than CRLs.

X.509 Standard

- The most common format used for digital certificates in PKI.
- Includes information like subject, issuer, public key, algorithm, and validity.

Key Pair (Public & Private Key)

- Public Key: Shared openly; used for encryption or verification.
- Private Key: Kept secret; used for decryption or signing

Examples:

Area	**Example**
Web Browsing	HTTPS websites with SSL/TLS certificates issued by CAs
Email Security	S/MIME and PGP for signing/encrypting emails
Secure Software Update	Operating systems verify update authenticity via signed certificates
Government e-Services	Digital ID cards, e-filing of taxes, e-voting
IoT Devices	Secure communication between sensors and gateways using certificates
Cloud Access	Azure AD, AWS IAM use PKI for access control and identity management

2. EXPLAIN THE COMMON CYBER ATTACKS

Cyber-Physical Systems (CPS) like healthcare devices, smart vehicles, industrial machinery, and IoT devices are vulnerable to various cyber-attacks due to insecure communication, limited authentication, and low processing power.

1. Man-in-the-Middle (MitM) Attack

- What It Is: An attacker intercepts and possibly alters the communication between two parties without their knowledge.
- How It Works: The attacker places themselves between a device and a hub (e.g., pacemaker and monitoring system).
- Impact in Healthcare: False data may be sent to doctors; attackers can impersonate devices.
- Real-world Risk: An attacker could send wrong vitals or commands to life-critical systems.

2. Information Harvesting

- What It Is: Unauthorized collection of personal, medical, or behavioural data from devices or networks.
- Why It Matters: Health data is extremely valuable on the black market (up to $50 per record).

Examples:

- Wearables like Fitbit showing when someone is away from home.
- Unmanned drones collecting video footage of private areas.
- Driverless cars storing sensitive route data.
- Risks: Identity theft, prescription leaks, extortion, or targeting high-profile individuals.

3. Denial-of-Service (DoS) Attack

- What It Is: Overloading or crashing a system to make it unavailable.

Tactics:

- Flooding networks with fake traffic.
- Sending high-power requests to drain battery-operated devices.
- Jamming signals between devices.
- Triggering magnetic switches in implanted medical devices to shut them off.
- Impact in CPS: Could affect vital functions like oil flow control, power generation, or hospital equipment.

Failure Modes:

- Fail-stop – system halts completely.
- Fail-safe – system enters a safe mode.
- Fail-loud – system sounds an alarm.
- Fail-quiet – system behaves normally but logs attack patterns for analysis.

4. Replay Attack

- What It Is: Capturing valid data from a network and resending it later to trick the system.
- Why It's Dangerous: Even if encrypted, repeated traffic can mislead devices or systems.
- Example: Replaying a command to open a medical drug dispenser or a smart lock.

Physical Security & Privacy Principles

- Physical and cyber security must work together in CPS. The interconnection makes attacks easier and defences harder to implement.

Key Principles:

Deterrence

- Warning signs, visible guards, or fences to scare off attackers.
- Example: Camera signage on hospital premises.

Detection

- Alarms or sensors that trigger when suspicious activity is detected.
- Example: Unauthorized access to a medical equipment room.

Delay

- Physical barriers (doors, locks) that slow down attackers.
- Example: Encrypted storage for patient data.

Response

- Immediate countermeasures (security personnel, system shutdown).
- Example: Auto-disabling compromised devices.

Neutralization

- Actions to render the attacker ineffective.
- Example: Blocking stolen certificates or access tokens.

Cyber + Physical Attack Paths in CPS

- The integration of cyber and physical systems increases attack surfaces.
- Vulnerabilities in either domain can compromise the whole system.
- Physical access can lead to cyber exploitation (e.g., plugging in malicious USB).
- Cyber access can control physical systems (e.g., hijacking an infusion pump).

Examples of CPS Attacks

Attack Point	**Example**
Device Interface	USB ports on hospital monitors
Network	Intercepting unencrypted Wi-Fi or Bluetooth traffic
Software Vulnerabilities	Flaws in firmware of wearable or implantable devices
Infrastructure	Compromised cloud servers storing patient data
Internet Access	Unsecured online APIs connecting hospital systems
User Behavior	Weak passwords or phishing attacks targeting doctors or patients