Cyber-Physical Systems (CPS) - 2 Mark Answers

---

1. Draw the diagram representing the workflow of the Cyber-Physical System

```
      CYBER-PHYSICAL SYSTEM WORKFLOW DIAGRAM


PHYSICAL WORLD
(Environment)

        Physical State


1. SENSORS
(Perception)

        Raw Data


2. COMMUNICATION
NETWORKS

        Digital Signals


3. COMPUTATION/PROCESSING
(Decision Making)
- Data Analysis
- Control Logic
- Optimization

        Control Commands


4. ACTUATORS
(Action Layer)

        Physical Action


PHYSICAL WORLD
```

```
    (Changed State)


                 Feedback (Closed Loop)
```

Key Elements: - **Sensing:** Sensors measure physical parameters continuously - **Communication:** Data transmitted through networks (WiFi, Ethernet, wireless) - **Processing:** Real-time computation and decision algorithms - **Actuation:** Commands executed by actuators (motors, pumps, valves) - **Feedback:** Closed-loop monitoring for continuous control

---

2. Briefly Explain Any Three Cyber Attacks in CPS

Attack 1: Denial of Service (DoS) Attack

- Attacker floods CPS network with excessive traffic or requests
- Overwhelms system resources (bandwidth, CPU, memory)
- Prevents legitimate users from accessing critical services
- **Consequence:** Loss of availability, system shutdown, operational disruption
- **Example:** Flooding SCADA server with network packets → power grid control unavailable

Attack 2: Man-in-the-Middle (MITM) Attack

- Attacker intercepts communication between control center and field devices
- Eavesdrops, modifies, or injects false control commands
- Compromises both confidentiality and integrity
- **Consequence:** Unauthorized control changes, corrupted sensor data
- **Example:** Intercepting pressure sensor readings in pipeline control system → attacker reads/modifies data

Attack 3: Malware/Ransomware Attack

- Malicious software injected into CPS systems
- Can steal data, encrypt files, or disable functionality
- Often delivered through phishing emails or vulnerable software
- **Consequence:** Complete system compromise, data breach, ransom demands
- **Example:** Ransomware infects industrial control system → encrypts critical files → system offline until ransom paid

---

3. Draw the Flowchart of the Context-Aware Biometric Security Framework

```
CONTEXT-AWARE BIOMETRIC SECURITY FRAMEWORK FLOWCHART


                START: User Authentication



              Collect Biometric Data
              (Fingerprint/Face/Iris)




              Extract Biometric Features
              (Template Generation)




              Collect Context Information
              • Time of Day
              • Location/Geolocation
              • Device Type
              • Network Type
              • User Behavior Pattern





              Risk Assessment Engine
              Calculate Risk Score


                Low Risk      High Risk



       Standard Auth          Multi-Factor Auth
       (Biometric Only)       (Biometric + OTP)
```

```
Verify Against Database
(Template Matching)

    Match      No Match

    GRANT       DENY
    ACCESS      ACCESS

Log Access Attempt
(Security Audit Trail)

    END: Update Security Status
```

Framework Components: - **Perception:** Biometric capture + context data collection - **Risk Assessment:** Dynamic risk scoring - **Adaptive Authentication:** Authentication level adjusts based on risk - **Decision:** Accept, Deny, or Request Additional Factors

---

4. Write About Any Three Characteristics of CPS

Characteristic 1: Real-Time Responsiveness

- CPS must respond to physical inputs within strict time constraints
- Deadlines are measured in milliseconds to microseconds
- Critical for safety applications where delays cause failures
- Requires deterministic timing and predictable behavior
- Example: Autonomous vehicle must brake within 50ms of obstacle detection

Characteristic 2: Integration of Physical and Cyber Components

- Seamless coupling between digital computation and physical processes
- Sensors continuously measure physical state → computation processes data → actuators change state

- Creates closed-loop feedback system
- Enables automatic control without human intervention
- Example: Medical ventilator adjusts airflow based on patient oxygen levels in real-time

Characteristic 3: Distributed and Heterogeneous Nature

- CPS typically comprises multiple interconnected devices across geographic locations
- Components may use different protocols, platforms, and technologies
- Requires interoperability and seamless coordination
- No central control point (resilient to failures)
- Example: Smart grid with distributed power plants, sensors, and control stations globally coordinated

---

5. Briefly Explain the Interception of SCADA Frames in CPS

What is SCADA? - Supervisory Control and Data Acquisition system for critical infrastructure (power grids, water systems, pipelines) - Transmits unencrypted or weakly encrypted control commands

Interception Process: - Attacker positions between SCADA control center and Remote Terminal Units (RTUs) - Captures network packets containing control frame data - Can observe real-time status information and analyze control commands - Often unencrypted, making data easily readable

Methods: - Packet sniffing using network analyzers - Man-in-the-middle proxy attacks - Network tapping on communication lines

---

6. Physical Consequences of SCADA Interception

Consequence 1: Equipment Damage

- Intercepted commands can manipulate actuators causing malfunction
- Pressure vessels rupture, pumps cavitate, transformers overheat
- **Impact:** Multi-million dollar equipment replacement

Consequence 2: Service Disruption

- Modified control signals shut down critical systems
- Power outages affecting thousands, water supply halted
- **Impact:** Loss of essential services, economic damage

Consequence 3: Safety Hazards

- Incorrect control signals cause explosions, fires, or personnel injury
- **Impact:** Loss of life, severe injuries, regulatory penalties

---

7. What are the Requirements of the Mitigation Model in CPS?

Functional Requirements:

1. Threat Detection & Prevention - Real-time anomaly detection mechanisms - Intrusion Detection Systems (IDS) monitoring network - Early warning systems for attacks - Automated response to threats

2. Access Control & Authentication - Multi-factor authentication for users and devices - Role-Based Access Control (RBAC) - Privilege escalation prevention - Credential management

3. Data Protection - End-to-end encryption for sensitive data - Secure key management - Data integrity verification (checksums, digital signatures) - Secure deletion of sensitive data

4. Secure Communication - Authenticated protocols (TLS/SSL) - Secure tunneling (VPN) - Input validation and output encoding - Protection against man-in-the-middle attacks

5. Incident Response - Automated incident response mechanisms - Isolation of compromised components - System recovery and restoration procedures - Forensic logging and analysis

Non-Functional Requirements:

6. Performance & Latency - Minimal overhead on real-time operations - Sub-millisecond security check latency - Scalable for large systems

7. Reliability & Availability - Fault tolerance and redundancy - 99.9% uptime requirement - Graceful degradation on failures

---

8. Write About the Three Main Components of Cyber-Physical System

Component 1: Physical Component (Plant)

- **Definition:** Actual devices, machinery, sensors, and actuators in the physical world
- **Includes:** Motors, valves, pumps, mechanical systems, physical sensors
- **Role:** Performs actual work and produces measurable outcomes

- **Example:** Assembly robot arm in factory, pump in water distribution system
- **Characteristics:** Subject to environmental factors, physical constraints, and wear

Component 2: Cyber Component (Computing and Control)

- **Definition:** Digital systems that process data and make control decisions
- **Includes:** Microprocessors, controllers, embedded systems, software algorithms
- **Role:** Analyzes sensor data, implements control logic, optimizes performance
- **Example:** Real-time controller calculating PID values, AI algorithm predicting failures
- **Characteristics:** Performs computation, makes decisions, implements policies

Component 3: Communication Component (Network)

- **Definition:** Infrastructure connecting physical and cyber components for data exchange
- **Includes:** Wired networks (Ethernet, CAN), wireless networks (WiFi, LoRaWAN, 5G), protocols
- **Role:** Enables sensor data transmission and control command delivery
- **Example:** Industrial Ethernet connecting sensors to PLC, WiFi in smart homes
- **Characteristics:** Must be reliable, secure, real-time capable, and low-latency

Integration: Physical sensors → Communication networks → Cyber processors → Communication networks → Actuators → Physical action

---

9. Write a Short Note on Deadlock

Definition: - Situation where two or more concurrent processes are blocked indefinitely - Each process waits for resource held by another process - System cannot proceed forward (mutual blocking)

Four Conditions for Deadlock (All Must Occur):

1. **Mutual Exclusion:** Resources cannot be shared; only one process uses at a time
2. **Hold and Wait:** Process holds allocated resources while waiting for others
3. **No Preemption:** Resources cannot be forcibly taken from processes

4. **Circular Wait:** Circular chain of processes each waiting for another's resource

Example:

```
Process A: Holds Resource 1, waits for Resource 2
Process B: Holds Resource 2, waits for Resource 1
→ Both blocked indefinitely (DEADLOCK)
```

Prevention Methods: - Acquire all resources together (eliminate hold and wait) - Allow preemption of resources - Avoid circular wait by ordering resource requests

Impact: System freeze, loss of functionality, requires restart

---

10. What is a Smart City?

Definition: - Urban environment integrating digital technology and data analytics with physical infrastructure - Uses IoT sensors, 5G networks, cloud computing for efficient city management

Key Components: - Smart transportation (traffic management, autonomous vehicles) - Smart utilities (electricity, water, gas distribution) - Smart buildings (automated HVAC, security, energy management) - Public safety (emergency response, crime prediction) - Environmental monitoring (air quality, pollution levels)

Benefits: - Reduced energy consumption (15-20% savings typical) - Improved traffic flow and reduced congestion - Better public services and emergency response - Environmental sustainability - Enhanced citizen quality of life

Example: Barcelona, Copenhagen, Singapore use smart city technologies for efficient urban management

---

11. Briefly Explain Any Three Cyber Consequences in CPS

Consequence 1: Data Breach and Information Disclosure

- Confidential data stolen by attackers
- Patient health records, industrial secrets, financial data exposed
- **Impact:** Loss of trust, regulatory fines (GDPR/HIPAA), competitive disadvantage
- **Example:** Hacker accesses patient database in connected healthcare system

Consequence 2: System Compromise and Loss of Control

- Attacker gains operational control of CPS
- Can issue unauthorized commands to actuators
- **Impact:** Unwanted physical actions, equipment damage, safety hazards
- **Example:** Ransomware encrypts power plant control system → operators cannot control generation

Consequence 3: Integrity Violation and Data Corruption

- Attackers modify sensor data or control signals
- System receives false information and makes wrong decisions
- **Impact:** Incorrect operations, cascading failures, safety violations
- **Example:** Attack modifies aircraft altimeter readings → pilot receives wrong altitude data

---

12. Write About the Perception Layer in CPS

Definition: - First layer of CPS responsible for sensing and acquiring physical world data - Acts as system's eyes and ears connecting physical environment to cyber system

Key Functions:

1. Sensing: - Sensors measure physical parameters (temperature, pressure, motion, light) - Continuous or event-triggered data collection - Multiple sensor types for comprehensive monitoring

2. Signal Conditioning: - Amplify weak sensor signals - Filter noise to improve accuracy - Convert analog signals to digital values

3. Data Acquisition: - Sample sensor data at appropriate rates - ADC (Analog-to-Digital) conversion - Buffer data for processing

4. Local Preprocessing: - Initial filtering and validation - Detect sensor faults and anomalies - Aggregate data from multiple sources

5. Quality Assurance: - Verify sensor accuracy and calibration - Detect stuck-at faults or drifting readings - Ensure data integrity

Components: - Sensors (temperature, pressure, motion, chemical, optical) - Signal conditioning circuits - ADC converters - Local microcontrollers - Data buffers

Example: In autonomous vehicle perception layer includes cameras, LiDAR, radar continuously monitoring road conditions

---

13. Briefly Explain About Attack Model in CPS

Definition: - Formal representation of potential threats and attack scenarios - Describes how attackers could compromise CPS security - Helps identify vulnerabilities and design defenses

Key Attack Models:

1. Threat Model: - Identifies who could attack (attacker profile) - What resources they have (capabilities) - What they can access (attack surface) - What their goals are (motivations)

2. Attack Vectors: - Possible paths attackers can exploit - **Network-based:** Cyber attacks via internet/intranet - **Physical-based:** Direct hardware tampering - **Social Engineering:** Tricking users into revealing credentials

3. Threat Scenarios: - Detailed descriptions of specific attack sequences - Example: Attacker gains access → installs malware → exfiltrates data → damages systems - Used to assess risk and design countermeasures

Components of Attack Model: - Attacker motivation and capability level - Attack surface (entry points) - Potential targets (assets at risk) - Consequences of successful attack - Detection and response mechanisms

Benefits: - Systematic security analysis - Identifies critical vulnerabilities - Guides security architecture design - Informs risk assessment and mitigation planning

---

14. List the Application Domains of CPS

Domain	Examples	Key Technologies
Transportation	Autonomous vehicles, traffic management, aircraft control	GPS, LiDAR, radar, vehicle-to-vehicle communication
Smart Grid	Power distribution, demand response, renewable integration	SCADA, phasor measurement, smart meters
Healthcare	Patient monitoring, medical devices, telemedicine	Biosensors, wireless networks, cloud platforms
Manufacturing	Robots, assembly lines, predictive maintenance	IoT sensors, AI/ML, edge computing

Domain	Examples	Key Technologies
Smart Cities	Traffic lights, utilities, buildings, public safety	Dense IoT networks, 5G, cloud analytics
Agriculture	Precision farming, crop monitoring, irrigation	Soil sensors, weather stations, drones
Aerospace	Flight control, autopilot, navigation systems	Redundant systems, real-time processing
Water Systems	Distribution, treatment, quality monitoring	Water quality sensors, automated control
Robotics	Industrial, surgical, service robots	Computer vision, real-time control, AI
Environmental	Pollution monitoring, disaster detection, climate monitoring	Sensor networks, satellite imagery, modeling

Key CPS Applications: - Autonomous vehicles and drones - Medical life-support systems - Industrial automation and predictive maintenance - Smart building energy management - Traffic and transportation management - Power grid optimization and control