Cyber-Physical Systems (CPS) - 3 Mark Answers

---

1. Discuss the Relation of Wireless Sensor Networks with Cyber-Physical Systems

Wireless Sensor Networks (WSN) form the **sensing and communication backbone** of CPS:

a) Perception Layer: - WSN collects real-time physical data (temperature, pressure, humidity) through distributed sensor nodes - Sensors transmit data wirelessly to CPS controllers using protocols like Zigbee, LoRaWAN, WiFi - Enables continuous environmental monitoring without human intervention

b) Communication Infrastructure: - WSN provides wireless connectivity reducing installation costs and enabling flexible deployment - Supports multi-hop communication extending network coverage - Creates low-latency communication channels between sensors, actuators, and decision-making systems

c) Scalability and Efficiency: - WSN architecture supports large-scale distributed systems (thousands of nodes across locations) - Edge computing at sensor nodes reduces bandwidth and latency - Energy-efficient protocols (sleep/wake scheduling) enable battery-powered remote operations - Cost-effective for monitoring inaccessible locations (forests, mountains, remote infrastructure)

Integration Example: Smart factory WSN monitors machinery vibration → transmits to CPS controller → triggers maintenance alerts and adjusts production parameters automatically.

Conclusion: WSN and CPS are symbiotic—WSN provides distributed sensing infrastructure that CPS depends on for real-time environmental perception and closed-loop control.

---

2. Explain CPS Hardware Platforms

CPS hardware platforms are embedded computing devices forming the computational foundation for real-time sensing and control.

Key Components:

a) Processors: - **Microcontrollers:** ARM Cortex-M (Arduino, STM32), Atmel ATmega - low power, GPIO pins, sensor interfaces - **Microprocessors:** ARM Cortex-A, Intel Atom - higher performance for complex processing - Provides real-time processing with deterministic timing

b) Memory System: - **Flash Memory:** Stores program code (non-volatile) - **RAM:** Runtime data storage (volatile) - **EEPROM:** Configuration storage (persistent)

c) Communication Interfaces: - **Wireless:** WiFi, Bluetooth, LoRaWAN, Zigbee, 5G/4G - **Wired:** CAN Bus (automotive), Ethernet, RS-232/485, I2C/SPI - Enables connectivity between sensors, controllers, and actuators

d) Analog/Digital Conversion: - **ADC:** Converts analog sensor signals to digital values - **DAC:** Converts digital control signals to analog output - **GPIO:** Digital I/O for device control

Popular Platforms:

Platform	Use Case	Features
Arduino Uno	Education, IoT	Easy programming, large community
Raspberry Pi 4	IoT, servers	Linux support, GPIO, connectivity
STM32F4	Industrial control	Real-time, 32-bit, ARM Cortex-M4
NVIDIA Jetson	AI/ML CPS	GPU acceleration, vision processing

e) Real-Time Operating System Support: - FreeRTOS, VxWorks, QNX enable deterministic task scheduling - Essential for safety-critical applications with strict timing deadlines

Conclusion: CPS hardware balances real-time responsiveness, low power consumption, cost efficiency, and reliability for deployment in demanding physical environments.

---

3. Explain the Steps in Risk Management

Risk management systematically identifies, analyzes, and mitigates threats to ensure CPS safety and security.

Step 1: Risk Identification - Enumerate all CPS assets (sensors, controllers, networks, actuators, data) - Identify threats (malware, physical attacks, network failures, hardware faults) - Discover vulnerabilities (unpatched software, weak passwords, poor encryption) - Methods: Expert interviews, vulnerability scanning, threat modeling, security audits - Output: Risk register listing all identified risks

Step 2: Risk Analysis - Assess **Likelihood** (High/Medium/Low): Probability of threat occurring - Estimate **Impact** (Critical/High/Medium/Low): Consequences if threat materializes - Calculate: **Risk = Likelihood × Impact** - Financial impact, safety impact, operational disruption assessed - Output: Risk analysis matrix showing all risks plotted by severity

Step 3: Risk Evaluation - Prioritize risks from highest to lowest severity - Define acceptance thresholds (Critical: > 80, High: 60-80, Medium: 40-60, Low: < 40) - Determine which risks require treatment vs. acceptance - Conduct cost-benefit analysis for mitigation - Output: Prioritized risk list with classifications

Step 4: Risk Mitigation - **Avoidance:** Eliminate risk by removing threat/vulnerability - **Reduction:** Implement controls (encryption, firewalls, access control, redundancy) - **Transference:** Transfer to third party (insurance, managed services) - **Acceptance:** Accept if mitigation cost exceeds benefit - Technical, administrative, and physical controls implemented - Output: Mitigation plan with timelines and responsible parties

Step 5: Monitoring & Review - Continuously monitor control effectiveness - Regular vulnerability scanning and patching - Re-assess risks quarterly or upon organizational changes - Track incidents and extract lessons learned - Update risk register as new threats emerge - Output: Updated risk register, metrics, incident reports

Cyclic Process: Risk management is continuous—new threats require return to identification step.

---

4. Write the Differences Between Physical Attack and Cyber Attack

Comparison Table

Aspect	Physical Attack	Cyber Attack
Definition	Direct physical tampering/damage of hardware	Exploitation of software/network vulnerabilities
Access Required	Physical proximity to equipment	Network connectivity (local or remote)
Visibility	Visible; requires on-site presence	Invisible; remote execution possible
Detection	Relatively easy (broken seals, damage)	Difficult; may go undetected for months
Execution Time	Slower (minutes to hours)	Very fast (milliseconds to seconds)
Cost	May be high (tools, resources)	Low/free (open-source tools available)
Attacker Type	Insider or local presence	Local or global remote attacker
Examples	Cut sensor wires, steal battery, smash device	SQL injection, malware, DDoS, brute force

Aspect	Physical Attack	Cyber Attack
Prevention	Locks, guards, tamper seals, surveillance	Firewalls, encryption, patches, MFA
Recovery	Hardware replacement/repair	Software patches, data restoration
Scope	Limited to equipment location	Affects distributed systems globally

Physical Attack Types:

- **Sensor Tampering:** Magnets near compass corrupting navigation; heating temperature sensor for false readings
- **Component Replacement:** Swapping genuine parts with malicious versions; installing fake firmware
- **Power Attacks:** Battery draining, cutting power supplies, overpower consumption devices
- **Cable Cutting:** Severing network or sensor cables causing disconnection
- **Physical Destruction:** Smashing, burning, dissolving components

Cyber Attack Types:

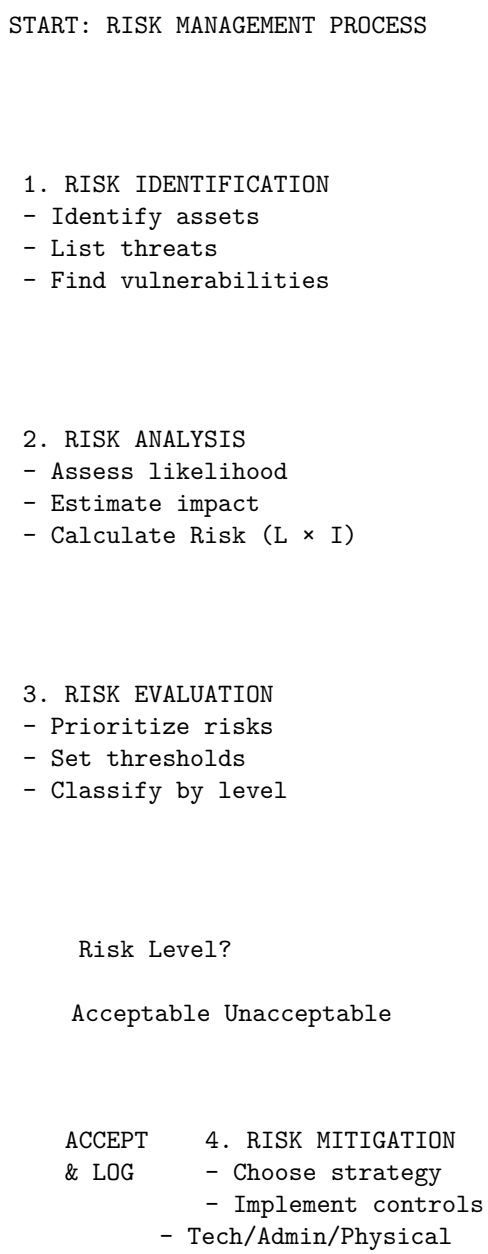
- **Malware:** Viruses, trojans, ransomware infecting systems
- **Network Intrusion:** Brute force password attacks, exploiting unpatched services
- **Data Manipulation:** Modifying sensor data or control commands in transit
- **Denial of Service (DoS):** Overwhelming system resources causing unavailability
- **Eavesdropping:** Intercepting sensitive communications without permission

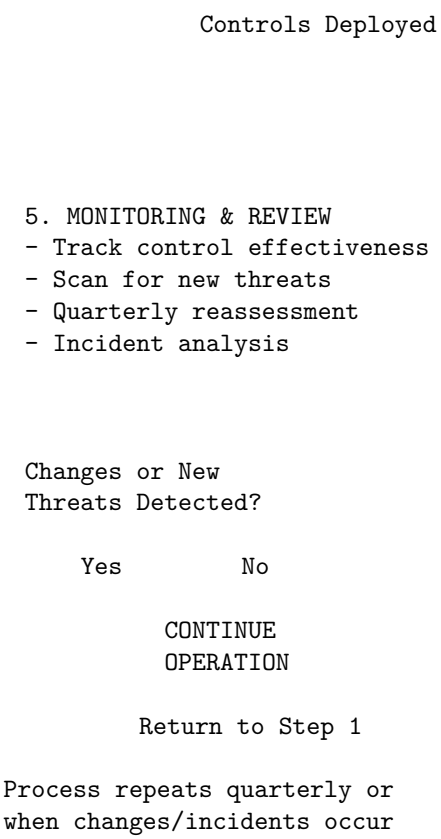
Key Differences:

- Physical attacks require **presence**, cyber attacks require only **connectivity**
- Physical attacks are **obvious**, cyber attacks are **subtle**
- Physical attacks have **localized impact**, cyber attacks can affect **global distributed systems**
- Physical security (locks) prevents physical attacks; cyber security (encryption, firewalls) prevents cyber attacks

---

5. Draw the Flowchart Explaining the Process of Risk Management





Key Decision Points: - **After Evaluation:** Acceptable risks proceed to monitoring; unacceptable risks require mitigation - **After Mitigation:** Verify controls implemented; begin monitoring - **During Review:** Identify new risks requiring return to identification step

---

6. Explain RTOS (Real-Time Operating System)

Definition: Specialized OS designed to execute tasks with predictable, deterministic timing to meet strict deadline constraints in real-time applications.

Key Characteristics:

a) Deterministic Behavior: - Guaranteed task execution within specified time windows - Predictable response time to events regardless of system load - Critical for safety-critical CPS (medical devices, aviation, autonomous vehicles)

b) Priority-Based Scheduling: - Tasks assigned priority levels (High/Medium/Low) - Higher priority tasks preempt lower priority ones - Ensures critical tasks

execute before non-critical tasks - Algorithms: Rate Monotonic Scheduling, Earliest Deadline First (EDF)

c) Low Latency: - Minimal delay from event to system response (microseconds to milliseconds) - Rapid context switching between tasks - Suitable for time-sensitive applications like emergency braking

d) Multitasking: - Multiple concurrent tasks/threads running independently - Each task has isolated execution context - Synchronization primitives (semaphores, mutexes) for shared resource access - Thread-safe operations

Types of RTOS:

Type	Guarantee	Use Case	Example
Hard Real-Time	Absolute deadline guarantee	Aircraft, life-support	VxWorks, QNX
Firm Real-Time	Occasional misses tolerable	Industrial automation	POSIX + RT extensions
Soft Real-Time	No guarantee, degradation acceptable	Multimedia, IoT	Linux with patches

Common RTOS Examples: - **FreeRTOS:** Open-source, lightweight, embedded IoT - **VxWorks:** Certified for safety-critical aerospace/automotive - **QNX:** Microkernel, excellent reliability, industrial - **INTEGRITY:** High security, real-time guarantees

Components: - Task scheduler for priority management - Context switching for task switching - Interrupt handler for event processing - Synchronization primitives for resource sharing - Device drivers for hardware control

Application in CPS: Medical ventilator must adjust airflow every 10ms based on patient sensors—RTOS ensures this timing deadline is always met.

---

7. Explain the Applications of Cyber-Physical Systems

CPS applications span critical infrastructure and consumer systems requiring real-time monitoring and control.

a) Smart Transportation: - Autonomous vehicles: LiDAR sensors → perception → control decisions → steering/braking - Adaptive cruise control: Radar detects vehicle distance → maintains set spacing - Traffic management: Sensors detect congestion → signal optimization - Benefits: Reduced accidents, improved traffic flow, fuel efficiency

b) Smart Grid and Power Systems: - Real-time monitoring of electrical distribution networks - Smart meters measure consumption; SCADA controls power flow - Integrates renewable energy (solar, wind) with demand management - Fault detection and self-healing capabilities - Benefits: Reduced outages, energy efficiency, grid stability

c) Industrial IoT (Industry 4.0): - Predictive maintenance: Vibration sensors detect equipment degradation before failure - Quality control: Computer vision inspects products automatically - Production optimization: Sensors adjust manufacturing parameters in real-time - Benefits: Reduced downtime, improved productivity, quality assurance

d) Healthcare and Medical Devices: - Remote patient monitoring: Wearable sensors track vital signs (heart rate, blood glucose) - Automated surgical robots: Minimally invasive surgery with precision - Smart hospitals: Automated medication dispensing, connected medical devices - Pacemakers: Wireless monitoring adjusts parameters based on patient condition - Benefits: Early disease detection, improved outcomes, reduced hospitalizations

e) Smart Cities: - Traffic lights synchronized using real-time traffic data - Smart lighting adjusts brightness based on time and traffic - Water systems detect leaks using pressure sensors - Waste management optimizes collection routes - Benefits: Reduced congestion, energy savings, better services

f) Precision Agriculture: - Soil moisture sensors guide irrigation decisions - Weather stations and crop cameras predict disease - Autonomous tractors perform planting/harvesting - Livestock tracking monitors animal health - Benefits: Increased yield, water conservation, reduced chemical usage

g) Environmental Monitoring: - Air quality sensors detect pollution levels - Earthquake early warning systems - Deforestation detection using satellite imagery - Volcano and tsunami monitoring - Benefits: Early disaster warning, environmental protection

h) Aerospace and Aviation: - Flight control systems maintain stability automatically - Air traffic control coordinates aircraft movements - Health management systems monitor aircraft systems - Predictive maintenance schedules maintenance before failures - Benefits: Enhanced safety, reduced accidents

Conclusion: CPS applications range from safety-critical aerospace to consumer IoT, enabling automation, efficiency, and improved quality of life.

---

8. Write the Differences Between Context-Aware Biometric Security Layer and Framework

Comparison Table

Aspect	Biometric Security Layer	Context-Aware Framework
Scope	Single component for biometric verification	Comprehensive multi-component security system
Context Awareness	No contextual consideration	Actively incorporates context data
Architecture	Single-layer implementation	Multi-layered (perception, analysis, decision, response)
Decision Making	Binary (match/no-match) or threshold-based	Risk-adaptive (dynamic requirements)
Authentication	Static requirements for all users	Adjusts based on risk assessment
User Experience	Consistent (always same process)	Adaptive (seamless low-risk, strict high-risk)
Threat Response	Same response to all attempts	Graduated responses (MFA, challenges, block)
Integration	Limited system integration	Integrates network, device, behavioral systems
Complexity	Simple single-purpose	Complex multi-subsystem architecture
Cost	Lower	Higher due to infrastructure

Biometric Security Layer:

Purpose: Verifies user identity based on unique biological characteristics

Process:

```
Biometric Input (fingerprint, face, iris)
        ↓
Feature Extraction (create template)
        ↓
Template Matching (compare against database)
        ↓
Similarity Score
        ↓
Decision: ACCEPT or REJECT (based on threshold)
```

Characteristics: - Stateless: Each authentication independent - Fixed threshold: Binary decision boundary - Limited information: Only biometric data - Cannot detect spoofing or unusual behavior patterns

Example: Employee swipes fingerprint—if 95% match, granted access regardless of location, time, or suspicious circumstances

Context-Aware Biometric Security Framework:

Purpose: Holistic security adapting authentication to contextual risk

Components: - Biometric sensors (fingerprint, face, voice, iris) - Context collectors (device, location, network, behavior) - Risk assessment engine (calculates risk score) - Adaptive decision engine (adjusts MFA requirements) - Response engine (grants access, requests MFA, or blocks)

Risk Assessment Factors: - **Temporal:** Time of day, location history patterns - **Geographic:** User location, travel time between logins - **Device:** Device type, security status, patch level - **Network:** WiFi/wired, IP reputation, VPN usage - **Behavioral:** User role, typical application usage, data access patterns

Authentication Adaptation: - **Low Risk (0-30):** Biometric only → seamless access - **Medium Risk (31-60):** Biometric + 2FA → SMS/OTP requested - **High Risk (61-85):** Multiple challenges → security questions + device verification - **Critical Risk (86-100):** Block immediately → alert security team

Example: - Low Risk: Employee logs in morning from home office—accepts fingerprint - High Risk: Unknown IP, 2 AM, foreign country—requests 2FA + security questions - Critical: Multiple failed attempts from blacklisted IP—blocks and alerts admin

Key Difference:

Layer answers "Is this biometric valid?" while Framework answers "Is this legitimate user in a legitimate context?"

---

9. Explain in Detail the Failures of CPS

CPS failures occur when systems don't perform intended functions due to hardware, software, communication, or security issues.

A. Hardware Failures:

Sensor Failures: - **Stuck-at-fault:** Reading frozen (temperature stuck at 25°C when actual 45°C) - **Drift:** Gradual measurement change over time - **Intermittent:** Occasional malfunctions - Consequences: Incorrect perception → wrong control decisions → system malfunction

Actuator Failures: - **Stuck-high:** Cannot deactivate (valve remains open) - **Stuck-low:** Cannot activate (brakes unresponsive) - **Partial response:** Sluggish actuation - Consequences: Loss of control over physical process

Processor/Controller Failure: - CPU crash, memory corruption, power supply failure - Results in complete system shutdown

Communication Hardware: - Cable damage, transceiver malfunction, port failure - Network disconnection preventing data transmission

B. Software Failures:

Logic Errors: - Incorrect control algorithms causing wrong actions - Example: Cooling disabled when temperature high (inverted logic) - Configuration errors with wrong parameters

Timing Issues: - Race conditions: Unpredictable behavior in concurrent tasks - Deadlock: Tasks block each other indefinitely - Priority inversion: Low-priority tasks blocking high-priority ones - Missed deadlines in real-time systems

C. Network/Communication Failures:

Message Loss: - Packet drops during transmission - Sensor data or control commands never arrive - Example: Power generation increase signal lost → power plant doesn't respond

Latency Issues: - Messages arrive too late for real-time control - Out-of-order delivery causing incorrect actions

Connectivity Loss: - Link failure, network partition - System disconnects from critical components

D. Safety-Critical Failures:

Loss of Containment: - Release of hazardous materials (chemical spill, radiation leak)

Control Loss: - Unable to steer, brake, accelerate - Emergency systems non-responsive

Integrity Compromise: - Structural damage, corrosion reducing component strength

E. Security-Induced Failures:

Cyber Attacks: - Malware infection compromising system - Unauthorized access allowing attacker control - Ransomware encrypting critical data

Example: Attacker compromises SCADA system → sends malicious commands → power transformers overload → grid blackout

Cascading Failures: - One component failure triggers chain reaction - Example: Sensor failure → wrong control signal → equipment damage → system shutdown

Impact Classification: - **Critical:** Safety hazard, service disruption, major damage - **High:** Degraded performance, recovery required - **Medium:** Noticeable impact, recoverable - **Low:** Minimal effect, transparent to users

---

10. Explain FCFS Scheduling Algorithm with an Example

First-Come-First-Served (FCFS) is a simple non-preemptive scheduling algorithm executing tasks in the order they arrive.

How FCFS Works:

Process: 1. Tasks enter ready queue in arrival order 2. CPU selects first task in queue 3. Task executes until completion (cannot be interrupted) 4. Next task in queue executes 5. Repeat until all tasks complete

Characteristics: - **Simple:** Easiest to implement - **Non-preemptive:** Once started, task runs to completion - **Fair:** All tasks get equal treatment - **Disadvantage:** Long tasks block short tasks (convoy effect)

Example:

Given Tasks: | Task | Arrival Time | Execution Time | Priority | |——|———————|————————-|———-| | T1 | 0 | 8 ms | - | | T2 | 1 | 4 ms | - | | T3 | 2 | 2 ms | - |

FCFS Execution Timeline:

```
Time: 0    8    12   14

Task:     T1    T2   T3


Timeline:
- T=0 to T=8:   T1 executes (8 ms)
- T=8 to T=12:  T2 executes (4 ms)
- T=12 to T=14: T3 executes (2 ms)
```

Performance Metrics:

Completion Time: - T1: 8 ms (arrives 0, completes 8) - T2: 12 ms (arrives 1, completes 12) - T3: 14 ms (arrives 2, completes 14)

Waiting Time: - T1: 0 ms (starts immediately) - T2: 7 ms (waits 1 to 8) - T3: 10 ms (waits 2 to 12) - **Average:** (0 + 7 + 10) / 3 = 5.67 ms

Turnaround Time: - T1: 8 ms - T2: 11 ms (completes at 12, arrived at 1) - T3: 12 ms (completes at 14, arrived at 2) - **Average:** (8 + 11 + 12) / 3 = 10.33 ms

Problem - Convoy Effect: If T1 takes 100 ms instead of 8 ms, T2 and T3 wait entire 100 ms even though they're short—inefficient!

Advantages: - Simple implementation - Fair (no starvation) - Suitable for batch processing

Disadvantages: - Poor average waiting time - Convoy effect (short tasks delayed by long tasks) - Not suitable for real-time systems - Doesn't consider task

priority

Better Alternatives for CPS: - **Shortest Job First (SJF):** Execute shorter tasks first - **Priority Scheduling:** Execute high-priority tasks first - **Round Robin:** Time quantum for each task

---

11. Discuss Smart Grid with a Perspective of CPS

Smart Grid is an intelligent electrical distribution network integrating sensing, communication, and control to optimize power generation, transmission, and consumption.

CPS Perspective - Key Components:

a) Sensors (Perception Layer): - **Smart Meters:** Measure residential/commercial electricity consumption - **Phasor Measurement Units (PMUs):** Monitor voltage, current, frequency in real-time - **Relay Sensors:** Detect faults and abnormal conditions - Collect continuous data from generation, transmission, and distribution points

b) Communication Network: - **SCADA:** Supervisory Control and Data Acquisition systems - **Advanced Metering Infrastructure (AMI):** Wireless meter reading - **5G/4G Networks:** Real-time control commands and data transmission - Enables coordination between power plants, substations, and consumers

c) Control Systems (Cyber Layer): - **Energy Management Systems:** Optimize load distribution - **Demand Response Systems:** Adjust consumption during peak hours - **Microgrid Controllers:** Manage distributed generation (solar, wind) - **Fault Detection:** Identify and isolate problems automatically - Real-time algorithms balance supply-demand

d) Actuators (Physical Layer): - **Switchgear:** Connect/disconnect power sources - **Voltage Regulators:** Adjust voltage levels - **Capacitor Banks:** Correct power factor - **Smart Transformer Taps:** Adjust transformation ratios - **Renewable Energy Converters:** Control solar/wind generation output

e) Feedback Loop:

```
Sensors (PMUs, meters) detect grid state
        ↓
Communication transmits data to control center
        ↓
Control algorithms analyze and decide
        ↓
Commands sent to actuators
        ↓
Switchgear/regulators adjust power flow
```

```
        ↓
Sensors monitor new state (closed loop)
```

Smart Grid Applications:

1. Load Balancing: - Distribute power demand across available generation capacity - Prevent overloading any transmission line - Shift non-critical loads to off-peak hours - Result: Reduced outages, improved stability

2. Renewable Integration: - Solar/wind generation is variable - CPS monitors renewable output and adjusts dispatch - Battery storage charged during excess generation - Example: Excess wind → charge EV batteries; low wind → discharge batteries

3. Demand Response: - During peak demand, reduce consumption automatically - Smart thermostats reduce temperature during peak hours - Water heaters charged during low-demand periods - Result: Reduced peak demand, lower costs

4. Fault Detection & Isolation: - Sensors detect line faults immediately - Automated switches isolate fault section - Reroute power through alternate paths - Results in: Faster restoration, fewer customers affected

5. Energy Efficiency: - Real-time consumption visibility for consumers - Dynamic pricing incentivizes off-peak usage - Outage prediction enables preventive maintenance - Result: 10-15% energy reduction

Real Example - Smart Grid Operation:

Scenario: Summer evening peak demand - 5 PM: Air conditioning demand surges - Sensors detect: Grid frequency dropping (supply $<$ demand) - Control system: Activates demand response - Actions: Thermostats raise temperature 1°C, water heater postpones heating, EV charging delayed - Result: Load reduced by 10%, frequency stabilized - All automatic with CPS—no manual intervention needed

Safety and Reliability:

Redundancy: - Multiple communication paths (if one fails, others work) - Backup power generation sources - Distributed intelligence (no single point of failure)

Real-Time Constraints: - Frequency regulation: Seconds - Fault detection: Milliseconds - Voltage control: Seconds - RTOS ensures all deadlines met

Conclusion: Smart Grid exemplifies CPS at scale—thousands of sensors continuously monitor electrical infrastructure, networked computers make real-time control decisions, and actuators implement changes to maintain stable, efficient power delivery. This integration of physical, computational, and communication systems defines modern smart grids.

---

12. Explain the Context-Aware Biometric Security Framework

Definition: A comprehensive, multi-layered security system that combines biometric verification with contextual data analysis to adaptively adjust authentication requirements based on real-time risk assessment.

Architecture:

```
CONTEXT-AWARE BIOMETRIC SECURITY FRAMEWORK


 Biometric Perception Layer
• Fingerprint sensor
• Face recognition camera
• Iris/retina scanner
• Voice recognition microphone


 Context Collection Layer
• Device info (type, security status)
• Location (GPS, WiFi triangulation)
• Network (IP, VPN, WiFi type)
• Time/behavior patterns
• Network behavior (connections)


 Risk Assessment Engine
Risk = Σ(Factor Weight × Anomaly)
• Biometric mismatch scoring
• Geographic impossibility detection
• Behavioral deviation analysis
• Device risk scoring


 Adaptive Decision Engine
• Low Risk: Accept biometric
• Medium Risk: Request 2FA
• High Risk: Challenge response
• Critical Risk: Block & Alert


 Response & Monitoring Layer
• Grant/deny access decision
• Session continuous monitoring
• Anomaly detection during session
```

- `Comprehensive audit logging`

Contextual Factors Considered:

1. Temporal Context: - Time of day (user normally logs 9 AM, now logging 2 AM = suspicious) - Day of week patterns - Seasonal access variations - User shift schedule (night shifts vs day workers)

2. Geographic Context: - User location (home, office, traveling) - Geolocation impossibility (logged in from two countries in 1 hour) - VPN/proxy usage - Known travel patterns

3. Device Context: - Device type (desktop, phone, tablet, laptop) - Device trust level (company vs personal device) - OS version and patch level - Security software installed (antivirus, firewall)

4. Network Context: - Network type (corporate vs public WiFi vs home) - IP address reputation - Proxy/VPN usage - Network security posture

5. Behavioral Context: - User role and department - Typical application usage - Data access patterns (which files accessed normally) - Peer group comparison (similar users' patterns)

Authentication Decision Example:

Scenario 1 - Low Risk: - Employee: Known accounts manager - Biometric: Face match 97% - Time: 9 AM Monday - Location: Home (known home IP) - Device: Company laptop - Behavior: Accessing usual finance application

Risk Score: 15/100 (Low) **Decision:** ACCEPT - Biometric only **User Experience:** Instant access

---

Scenario 2 - Medium Risk: - Employee: Known accounts manager - Biometric: Fingerprint 94% - Time: 1 AM Wednesday - Location: Airport - Device: Personal phone - Behavior: Accessing new high-value transaction reports

Risk Score: 55/100 (Medium) **Decision:** REQUEST 2FA **Action:** Send OTP to registered phone **User Experience:** Brief security check

---

Scenario 3 - High Risk: - Employee: Known accounts manager - Biometric: No match - Time: 3 AM - Location: Foreign country (impossible travel time) - Device: Unknown device - Behavior: Multiple failed attempts + access to sensitive employee records

Risk Score: 82/100 (High) **Decision:** BLOCK & CHALLENGE **Actions:** - Request security questions - Notify account owner - Alert security team **User**

Experience: Denied access, investigation

Scenario 4 - Critical Risk: - Unknown user - Biometric: No registered match - Time: Midnight - Location: Blacklisted IP address - Device: Unrecognized, outdated OS - Behavior: Brute force attempts, SQL injection attempts

Risk Score: 98/100 (Critical) **Decision:** BLOCK IMMEDIATELY **Actions:** - Account lockdown - Disable IP address access - Alert security operations center - Trigger incident response **User Experience:** Access denied, security investigation

Key Benefits:

1. **Adaptive Security:** Seamless for legitimate users, strict for suspicious access
2. **Real-Time Risk:** Dynamic assessment not static rules
3. **Multi-Factor:** Combines biometric + context for strong security
4. **Anomaly Detection:** Identifies unusual behavior patterns
5. **Reduced False Positives:** Context explains legitimate variation
6. **User Experience:** High-trust scenarios require minimal friction
7. **Compliance:** Audit trail for regulatory requirements

Continuous Monitoring During Session: - Ongoing behavioral verification (keystroke dynamics, mouse movement) - Anomalous application access triggers re-authentication - Timeout based on risk level (low-risk: longer timeout) - Automatic session termination on high-risk detection

Conclusion: Context-aware biometric security framework provides enterprise-grade security by adapting authentication rigor to real-time risk assessment, balancing security and usability.