Implementing IoT in Manufacturing

Program code: UNINMU11

Implementing IoT in Manufacturing

Learning Objective:

Understand the principles and processes of implementing IoT in manufacturing, focusing on machine-to-machine (M2M) communication and effective data collection

Learning Outcomes:

- Role of IoT in enhancing operational efficiency & automation in manufacturing
- Identify key components & technologies involved in IoT-based data collection systems
- Develop a basic implementation plan for integrating IoT systems into existing manufacturing processes

Implementing IoT in Manufacturing

Learning Objectives:

- Fundamentals of IoT and its impact on manufacturing
- Integration of IoT with manufacturing systems
- Benefits and challenges of IoT implementation

Application of concepts:

- **Examples**: The IoT Transformation of Technocraft Industries, Norsk Hydro, a major aluminum producer, response to a ransomware attack
- **Case Study**: Harley-Davidson's IoT-Driven Production Efficiency Improvement
- **Simulation**: Designing and Implementing an IoT-Enabled Smart Factory Production Line
- **Role Play**: Simulate a board meeting to decide on the next steps for Harley-Davidson’s digital transformation

Case Study: Harley-Davidson's IoT-Driven Production Efficiency Improvement https://docs.google.com/document/d/1UZziBq7ZjyYz6jQqMXJVrKCAukuDKSUClDxXLliHC70/edit

Pre read for the session

1. Technical Architecture of your org. IT setup - protocols and standards
2. List of various machines - Rank order of Criticality and importance in production
3. Functioning of security operations center (SOC) at your org - procedures for responding to various types of cyber threats, Server backup and restore process, patching process for Control System equipment, SCADA etc.
4. Case Study: Harley-Davidson's IoT-Driven Production Efficiency Improvement https://docs.google.com/document/d/1UZziBq7ZjyYz6jQqMXJVrKCAukuDKSUClDxXLIiHC70/edit

Required during session

1. Interest in Industrial IoT
2. Laptops/tablets with internet access (optional for research activities)
3. Whiteboard or flip charts for group discussions
4. Markers, pens, and paper for notes

ZEN LEARN

Learning Objective 1

Basics of IoT in the manufacturing context

Skill Sets to acquire:
IoT, IoT Architecture, IoT Protocols

Core Concepts

- IoT Architecture in Manufacturing
- IoT Protocols in Manufacturing
- Factors to Consider When Choosing Architecture and Protocols

IoT Architecture in Manufacturing

IIoT platforms enable enhanced machine-to-machine (M2M) communication and data collection, leading to smarter, more efficient operations. By connecting industrial equipment and systems through a network of sensors, actuators, and intelligent devices, IIoT platforms collect and exchange data, transform raw data into actionable insights, to optimize processes, improve efficiency, and reduce costs.

IoT devices and sensors are used in automotive manufacturing plants to monitor the condition of machines, track parts through the supply chain, and optimize energy use.

IoT architecture in manufacturing typically consists of several layers, each playing a critical role in the flow of data and control throughout the system. The most common architecture is layered into four key levels: the perception layer, network layer, processing layer, and application layer.

A. Perception Layer (Device Layer) lowest layer in the IoT architecture, where data collection occurs. It involves physical devices and sensors that monitor various parameters such as temperature, pressure, humidity, vibration, and machine status.

- **Components:**
  - **Sensors and Actuators:** Devices that collect data and perform actions based on control signals.
  - **Embedded Systems:** Microcontrollers or microprocessors integrated into machinery for local data processing.
  - **Examples:** Temperature sensors on CNC machines, vibration sensors on motors, RFID tags for inventory tracking.

IoT Architecture in Manufacturing

B. Network Layer (Connectivity Layer) for transmitting the collected data from the perception layer to the processing layer. It also handles the communication between devices within the manufacturing plant.

- **Components:**
  - **Communication Protocols:** such as MQTT, HTTP, CoAP, & WebSockets enable data transmission over the network
  - **Gateways:** Devices that aggregate data from multiple sensors & translate it into protocols that can be understood by the network
  - **Examples:** Wi-Fi, Ethernet, Zigbee, LoRaWAN, and 5G for high-speed, reliable data transmission.

C. Processing Layer (Data Management Layer) collected data is processed, stored, & analyzed

- **Components:**
  - **Edge Devices:** Localized computing devices that process data near the source to reduce latency & bandwidth usage
  - **Cloud Platforms:** Centralized platforms that provide scalable processing power, storage, & advanced analytics
  - **Examples:** AWS IoT Core, Microsoft Azure IoT Hub, IBM Watson IoT Platform.

D. Application Layer user interface & specific business logic for monitoring, controlling, & optimizing manufacturing processes. It translates raw data into actionable insights

- **Components:**
  - **Applications:** Software applications that visualize data, provide analytics, and support decision-making.
  - **APIs:** Application Programming Interfaces that enable integration with other business systems like ERP or MES.
  - **Examples:** Predictive maintenance platforms, real-time monitoring dashboards, digital twins.

IoT Protocols in Manufacturing

IoT protocols are essential for enabling communication between devices and systems in a manufacturing environment. These protocols ensure that data is transmitted efficiently, reliably, and securely across the network. Some key protocols are below:

A. MQTT (Message Queuing Telemetry Transport)

- **Overview:** MQTT is a lightweight messaging protocol designed for low-bandwidth, high-latency networks. It operates on a publish-subscribe model. Devices (clients) subscribe to topics, and messages are published to these topics by other devices.
- **Use Case in Manufacturing:** MQTT is widely used in scenarios where low-power devices need to communicate over unreliable networks, such as remote monitoring of equipment in large manufacturing plants.
- **Benefits:** Low bandwidth usage, simplicity, and scalability.

B. CoAP (Constrained Application Protocol)

- **Overview:** CoAP is a protocol designed for constrained devices that operate in low-power, low-bandwidth environments. It is similar to HTTP but optimized for IoT with a smaller packet size and lower overhead.
- **Use Case in Manufacturing:** CoAP is used in applications like smart sensors and actuators that require efficient data transmission in constrained environments.
- **Benefits:** Low power consumption, efficient communication in resource-constrained environments.

C. OPC UA (Open Platform Communications Unified Architecture)

- **Overview:** OPC UA is a machine-to-machine communication protocol for industrial automation. It provides a framework for secure and reliable data exchange between machines, devices, and systems.
- **Use Case in Manufacturing:** OPC UA is widely adopted in industrial automation for connecting PLCs, SCADA systems, and other industrial control systems with IoT platforms.
- **Benefits:** Interoperability, security, and scalability in industrial environments.

Example - Indian / global financial firm

D. HTTP/HTTPS (Hypertext Transfer Protocol)

- **Overview:** HTTP is the foundational protocol of the WWW, used for transmitting hypertext. In IoT, it's used for RESTful APIs and web-based communication between devices and servers
- **Use Case in Manufacturing:** HTTP(S) is used in web-based interfaces for IoT, ie. remote monitoring dashboards & control systems
- **Benefits:** Ubiquity, ease of use, and support for secure communication via HTTPS

E. Zigbee

- **Overview:** Wireless communication protocol based on IEEE 802.15.4 standard, for low-power, low-data-rate communication over short distances
- **Use Case in Manufacturing:** Sensor networks for monitoring environmental conditions or tracking inventory
- **Benefits:** Low power consumption, mesh networking capabilities, and cost-effectiveness

F. LoRaWAN (Long Range Wide Area Network)

- **Overview:** LoRaWAN is a low-power, wide-area networking protocol designed for battery-operated devices in large-scale deployments
- **Use Case in Manufacturing:** Ideal for applications like asset tracking & environmental monitoring across large industrial sites
- **Benefits:** Long-range communication, low power consumption, and scalability for large networks

G. Modbus

- **Overview:** Serial communication protocol widely used in industrial settings for communication between devices over serial lines (RS-232, RS-485) or Ethernet
- **Use Case in Manufacturing:** To connect PLCs and other industrial equipment with IoT gateways or SCADA systems
- **Benefits:** Simplicity, reliability, and widespread adoption in industrial environments

Common Architectures & Protocols and Their Applications

Architecture/ Protocol	Best Suited For	Key Features	Typical Applications	Considerations
Modbus	Small to medium-sized plants, simple data exchange	Easy to implement, cost-effective	Basic monitoring, device communication	Limited scalability, not for high-speed operations
OPC UA	Medium to large plants, cross-platform integration	Secure, platform-independent, supports complex data	SCADA, cross platform integration, data aggregation	Requires more processing power, complexity in setup
EtherNet/IP	Large plants, high-speed, real-time operations	High bandwidth, real-time capabilities, widely used in industrial automation	Robotics, CNC machining, process control	Requires robust network infrastructure, higher cost
PROFINET	High-speed, deterministic communication	High-speed, deterministic, supports large-scale automation	Factory automation, motion control, high precision mfg	Complex to configure, higher cost
EtherCAT	Ultra-fast communication, real-time control	Ultra-low latency, high synchronization	Robotics, motion control, CNC machines	Requires precise setup, typically more expensive
MQTT	Data collection, cloud integration, IoT	Lightweight, supports low bandwidth, efficient data transfer	Predictive maintenance, remote monitoring	Not real-time, security depends on implementation
CANopen	Small-scale, reliable communication	Reliable, robust, low-cost	Automotive, simple automation systems	Limited scalability, not suited for high data volumes
Wireless (Wi-Fi, Zigbee, LoRaWAN)	Flexible deployment, mobile applications	Flexible, easy to deploy, supports remote monitoring	Mobile robots, AGVs, remote sensors	Potential interference, security concerns

Example: The IoT Transformation of Technocraft Industries

In 2019, Technocraft Industries (India) Ltd. Mumbai, known for precision-engineered products, operated with several standalone systems for production tracking, inventory management, & machine monitoring. It has CNC machines for precision manufacturing, injection molding machines, Warehouse management systems & production tracking systems. These systems were not integrated.

Machine downtimes and suboptimal material flow caused bottlenecks in the production process, affecting overall efficiency. Excess inventory was maintained to compensate for production scheduling uncertainties, tying up capital & incurring storage costs. Management relied on historical data, leading to delays in adjusting production schedules & responding to market demands. The company's management, led by CEO Mr. Rahul Gupta, recognized that to stay competitive, Technocraft needed to modernize its operations. The transformation journey was a data-driven approach.

Step 1: Assessing the Current State and Identifying Gaps: TCS conducted a comprehensive assessment. The assessment revealed that the company's existing IT infrastructure was outdated and lacked the capacity for real-time data processing & integration. The machines were operating independently, without any central monitoring or optimization.

Step 2: Choosing the Right IoT Architecture and Protocols: TCS recommended a hybrid IoT architecture combining edge computing for real-time data processing at the machine level and cloud computing for data storage, analytics, and long-term decision-making.

OPC UA protocol standardize communication between equipment, ensuring interoperability. MQTT was used for communication between edge devices and the cloud platform. EtherNet/IP protocol was used for real-time communication between critical machines and the central control system.

Example: The IoT Transformation of Technocraft Industries

Step 3: Upgrading Machines and Systems: ₹80 Lac (~$110,000) was invested in upgrading CNC machines with IoT sensors and edge computing devices. These upgrades enabled real-time monitoring of machine health, tool wear, and production output.

₹50 Lac (~$70,000) was spent on retrofitting Injection Molding Machines machines. ₹30 Lac (~$40,000) was invested in enhancing the assembly lines with IoT connectivity and centralized control systems. ₹20 Lac (~$27,000) was used to upgrade the WMS with IoT-enabled inventory tracking, allowing for real-time visibility into stock levels and automated reorder alerts.

Step 4: Implementing and Integrating Systems: A cloud-based analytics platform was implemented for monitoring production, inventory, and machine performance. IoT platform was integrated with existing ERP for data flow across departments.

Results After Modernization:

- **Inventory Reduction:** Inventory levels decreased by 20% (industry benchmark 15-25%), freeing up capital that had previously been tied up in excess stock. This reduction was primarily due to real-time inventory tracking and demand forecasting enabled by the IoT-enabled WMS.
- **Production Efficiency:** Production efficiency improved by 25% (industry benchmark 20-30%), as real-time monitoring optimized material flow and predictive maintenance reduced machine downtimes
- **Decision-Making Speed:** With real-time data available through the cloud-based analytics platform, decision making is faster.
- **Cost Savings:** The company achieved overall operational cost savings of ₹1 Crore (~$135,000) in the first year after the IoT upgrades, primarily due to reduced machine downtime, optimized energy usage, and lower inventory costs, achieved an ROI of approximately 200% within the first two years.

Common follow-up questions

1. What are the key components of an IoT architecture in a manufacturing environment, and how do they interact?
2. How do different IoT protocols impact the efficiency and security of a manufacturing system?
3. What factors should be considered when selecting an IoT architecture for a specific manufacturing process?
4. How do edge computing and cloud computing fit into the IoT architecture in manufacturing?
5. What are the most common challenges when implementing IoT protocols in a manufacturing setting, and how can they be addressed?

Assessment

Assignment 1

Which layer of the IoT architecture is responsible for processing and analyzing data?

a) **Device layer**

b) **Communication layer**

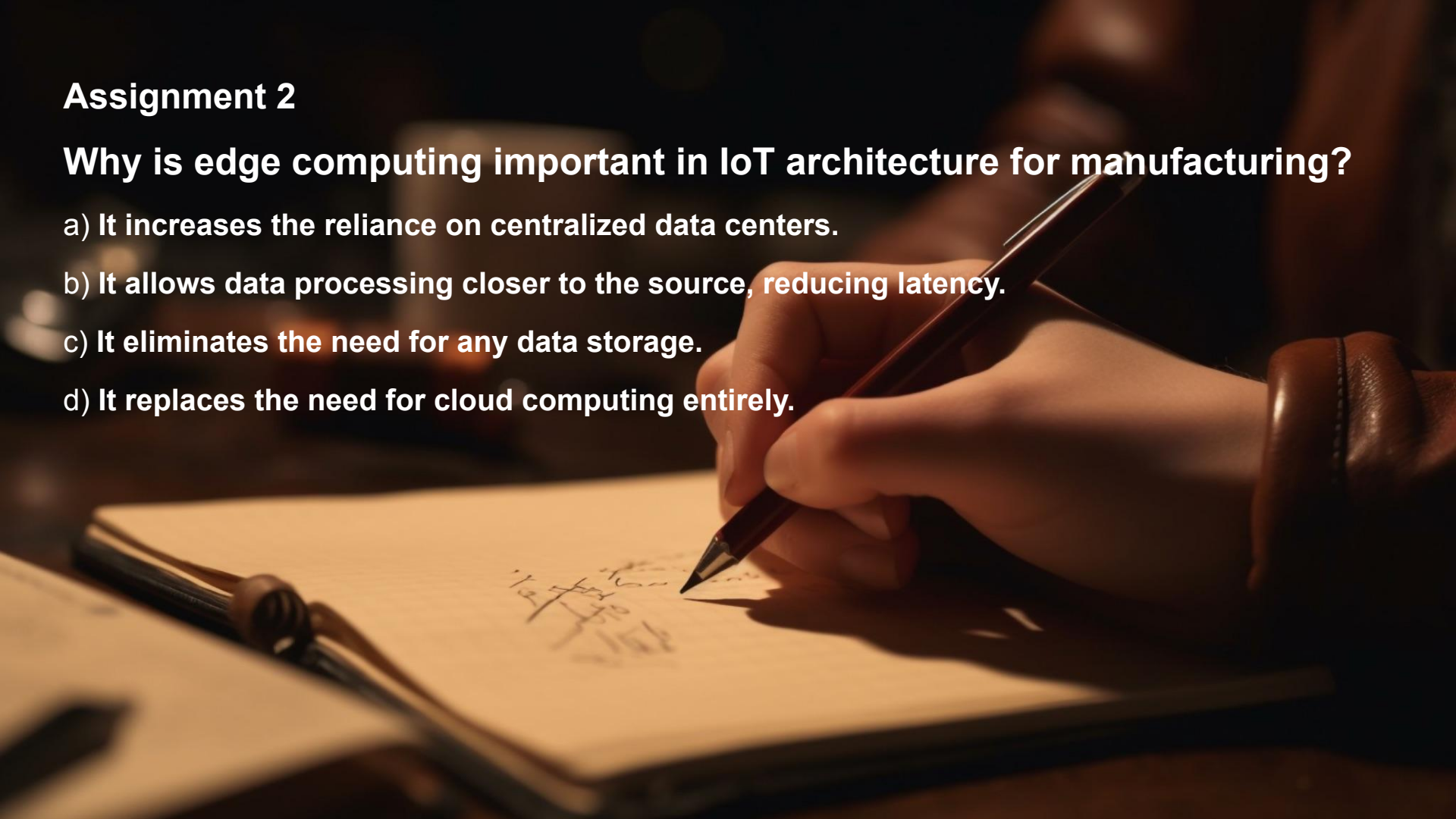
c) **Application layer**

d) **Perception layer**

Explanation Assignment 1

Correct Answer: c) **Application layer**

- **Explanation for Incorrect Options:**
  - **a) Device layer:** This layer involves sensors and devices collecting data, not processing it.
  - **b) Communication layer:** This layer handles the transmission of data between devices and the cloud, not the processing.
  - **d) Perception layer:** This is the physical layer where data is generated through sensors, not where it is analyzed.



Assignment 2

Why is edge computing important in IoT architecture for manufacturing?

a) **It increases the reliance on centralized data centers.**

b) **It allows data processing closer to the source, reducing latency.**

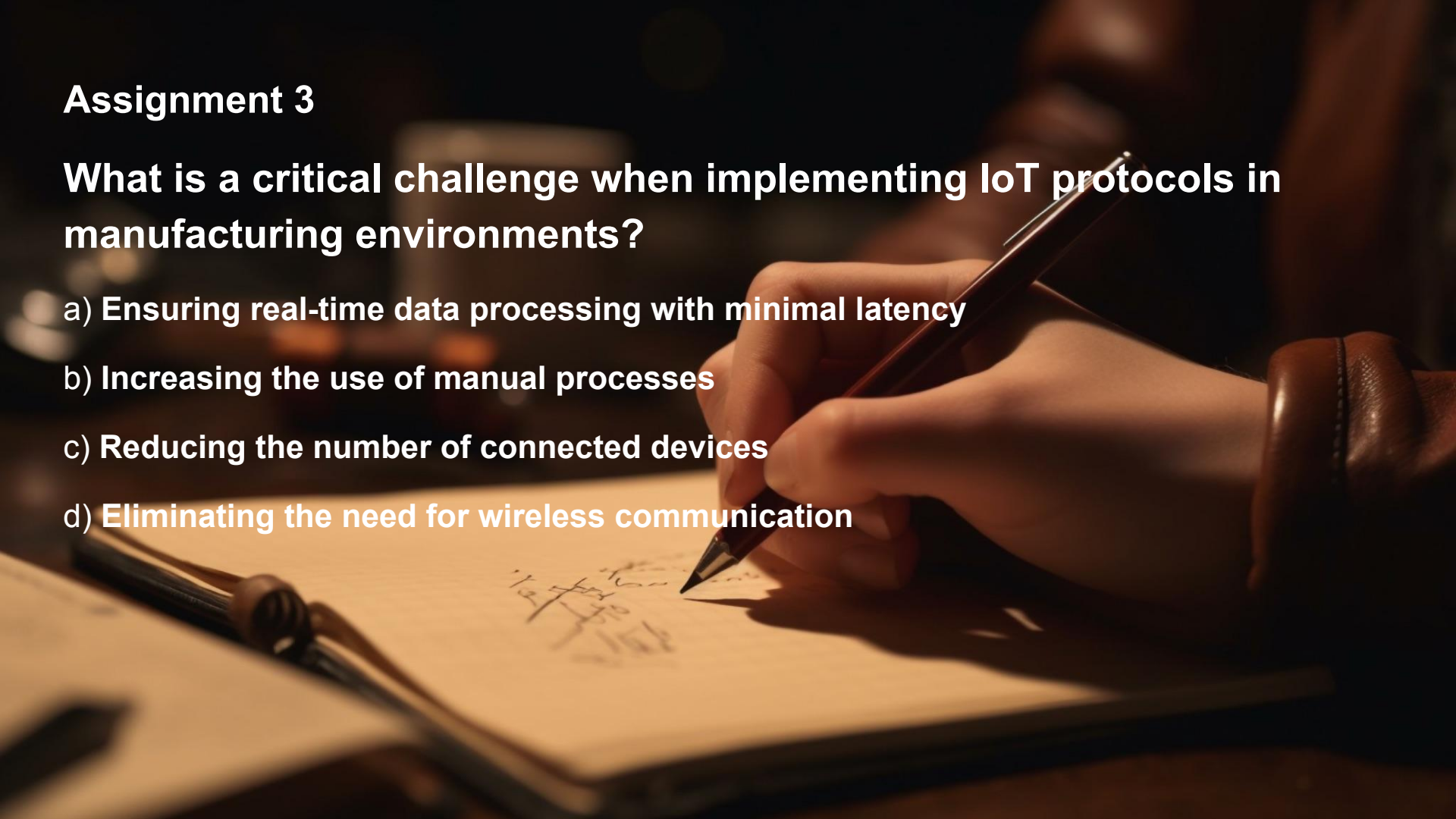
c) **It eliminates the need for any data storage.**

d) **It replaces the need for cloud computing entirely.**

Explanation Assignment 2

Correct Answer: b) **It allows data processing closer to the source, reducing latency.**

- **Explanation for Incorrect Options:**
  - **a) It increases the reliance on centralized data centers:** Edge computing reduces reliance on centralized data centers by processing data locally.
  - **c) It eliminates the need for any data storage:** Data storage is still needed, both locally and in the cloud, for comprehensive IoT solutions.
  - **d) It replaces the need for cloud computing entirely:** Edge computing complements cloud computing by handling time-sensitive data locally.



Assignment 3

What is a critical challenge when implementing IoT protocols in manufacturing environments?

a) **Ensuring real-time data processing with minimal latency**

b) **Increasing the use of manual processes**

c) **Reducing the number of connected devices**

d) **Eliminating the need for wireless communication**

Explanation Assignment 3

Correct Answer: a) **Ensuring real-time data processing with minimal latency**

- **Explanation for Incorrect Options:**
  - **b) Increasing the use of manual processes:** IoT aims to automate and reduce manual processes.
  - **c) Reducing the number of connected devices:** IoT systems thrive on connectivity; reducing connected devices is contrary to its purpose.
  - **d) Eliminating the need for wireless communication:** Wireless communication is a fundamental aspect of IoT, not something to be eliminated.

Assignment 4

Which IoT protocol is designed specifically for constrained devices with limited processing power?

a) **CoAP (Constrained Application Protocol)**

b) **HTTP**

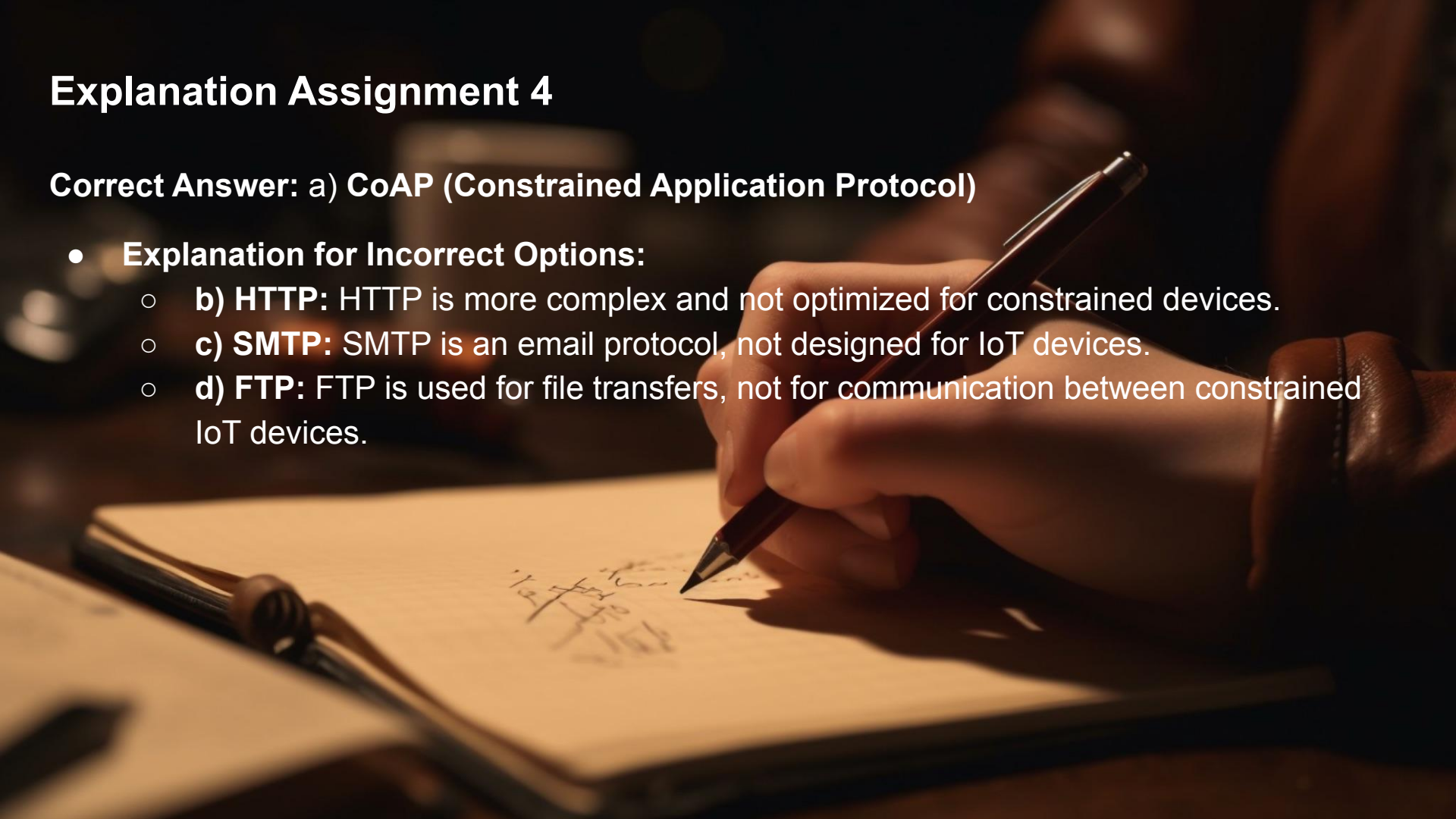
c) **SMTP**

d) **FTP**

Explanation Assignment 4

Correct Answer: a) **CoAP (Constrained Application Protocol)**

- **Explanation for Incorrect Options:**
  - **b) HTTP:** HTTP is more complex and not optimized for constrained devices.
  - **c) SMTP:** SMTP is an email protocol, not designed for IoT devices.
  - **d) FTP:** FTP is used for file transfers, not for communication between constrained IoT devices.



Assignment 5

What is one reason why MQTT is often used in manufacturing IoT applications?

- a) **It uses a lot of bandwidth.**
- b) **It is lightweight and efficient for low-bandwidth environments.**
- c) **It is specifically designed for video streaming.**
- d) **It requires frequent human intervention.**

Explanation Assignment 5

Correct Answer: b) **It is lightweight and efficient for low-bandwidth environments.**

- **Explanation for Incorrect Options:**
  - **a) It uses a lot of bandwidth:** MQTT is designed to be lightweight and minimize bandwidth usage.
  - **c) It is specifically designed for video streaming:** MQTT is designed for messaging between devices, not for video streaming.
  - **d) It requires frequent human intervention:** MQTT is designed to operate with minimal human intervention, making it ideal for IoT applications.

ZEN LEARN

Learning Objective 2

Integration of IoT with manufacturing systems

Skill Sets to acquire:
Machine-to-Machine (M2M) Communication, Data Collection, Interoperability, Sensor Integration

Core Concepts

- Components of IIoT platform
- Enhancing Machine-to-Machine (M2M) Communication
- Enhancing Data Collection and Utilization

Components of IIoT platform

IIoT platforms are integrated systems that connect various devices, machines, and sensors within an industrial environment. These platforms serve as the backbone for managing and analyzing the vast amounts of data generated by connected devices. An IIoT platform typically consists of the following components:

- **Device Management:** Tools for managing and monitoring connected devices, ensuring they function correctly and securely.
- **Connectivity Management:** The infrastructure that facilitates communication between devices, including network protocols, gateways, and communication standards.
- **Data Management:** Systems that collect, store, process, and analyze data generated by devices, transforming it into useful information.
- **Application Enablement:** Software tools and APIs that allow developers to create custom applications and dashboards that utilize the collected data.
- **Security:** Measures to protect data and devices from unauthorized access and cyber threats.

Enhancing Machine-to-Machine (M2M) Communication

M2M communication is at the core of IIoT, enabling machines to interact directly with each other without human intervention.

A. Real-Time Data Exchange

- **Low Latency Communication:** IIoT platforms enable low-latency communication between machines, allowing for real-time data exchange and decision-making. This is crucial in applications like predictive maintenance, where immediate responses to data anomalies can prevent equipment failures.
- **Example:** Sensors on a conveyor belt detect a temperature rise in a motor. The IIoT platform instantly communicates this data to the control system, which can then adjust the motor speed or trigger maintenance alerts without delay.

B. Interoperability Between Different Systems

- **Standardized Protocols:** IIoT platforms support a wide range of communication protocols, ensuring that machines from different manufacturers can communicate effectively. Protocols like OPC UA, MQTT, and Modbus are commonly used to enable interoperability.
- **Example:** An IIoT platform ensures robots from different vendors on assembly line can communicate and coordinate their actions, even though they use different control systems and communication protocols.

C. Autonomous Operations

- **Edge Computing:** IIoT platforms often incorporate edge computing, which allows data processing to occur close to the source (i.e., the machines themselves). This reduces the need for constant communication with a central server, enabling machines to operate autonomously based on real-time data.
- **Example:** In a smart grid, sensors distributed across the network monitor power usage and automatically adjust generation levels to balance supply and demand, all managed by the IIoT platform without human intervention.

Enhancing Data Collection and Utilization

IIoT platforms are powerful tools for collecting and improving processing of vast amounts of data from connected devices.

A. Comprehensive Data Collection

- **Sensor Integration:** IIoT platforms integrate data from a variety of sensors, including temperature, pressure, vibration, and more. This comprehensive data collection allows for a detailed understanding of machine health and performance.
- **Example:** In a chemical processing plant, sensors monitor variables like pressure, temperature, & flow rates across different reactors. The IIoT platform collects this data in real-time, enabling operators to optimize production processes & ensure safety

B. Data Aggregation and Processing

- **Centralized Data Storage:** IIoT platforms aggregate data from multiple machines & stores in centralized database or cloud platform. This centralization makes it easier to analyze data holistically, identifying trends & patterns.
- **Example:** A wind farm uses IIoT to collect data from all its turbines. By aggregating this data, the platform can analyze performance across the entire farm, identifying which turbines are underperforming and why.

C. Advanced Analytics and Machine Learning

- **Predictive Maintenance:** IIoT platforms use advanced analytics & ML to predict when machines are likely to fail, based on historical & real-time data. This allows for maintenance to be performed just in time, reducing downtime & maintenance costs
- **Example:** In an automotive assembly line, IIoT data analytics predict the wear and tear of welding robots. Maintenance is scheduled only when necessary, avoiding unnecessary service interruptions and extending the robots' operational life.

D. Real-Time Monitoring and Alerts

- **Dashboards and Alerts:** IIoT platforms provide real-time monitoring dashboards that display key performance indicators (KPIs) and send alerts when thresholds are breached. This enables swift responses to potential issues.
- **Example:** In a power plant, operators use an IIoT dashboard to monitor equipment status. If a turbine's vibration level exceeds safe limits, the platform sends an instant alert, prompting immediate inspection and potentially preventing a catastrophic failure

Common follow-up questions

1. What are the key components of an Industrial IoT (IIoT) platform, and how do they integrate with existing manufacturing systems?
2. How does enhancing Machine-to-Machine (M2M) communication improve efficiency and reduce downtime in manufacturing?
3. What are the best practices for collecting and utilizing data from IIoT-enabled devices in a manufacturing environment?
4. How can IIoT platforms help in predictive maintenance and real-time monitoring of manufacturing processes?
5. What challenges might arise when integrating IIoT with legacy manufacturing systems, and how can they be addressed?

Assessment

Assignment 1

Which of the following is a critical component of an Industrial IoT (IIoT) platform?

a) **Standalone manual workstations**

b) **Edge devices and gateways**

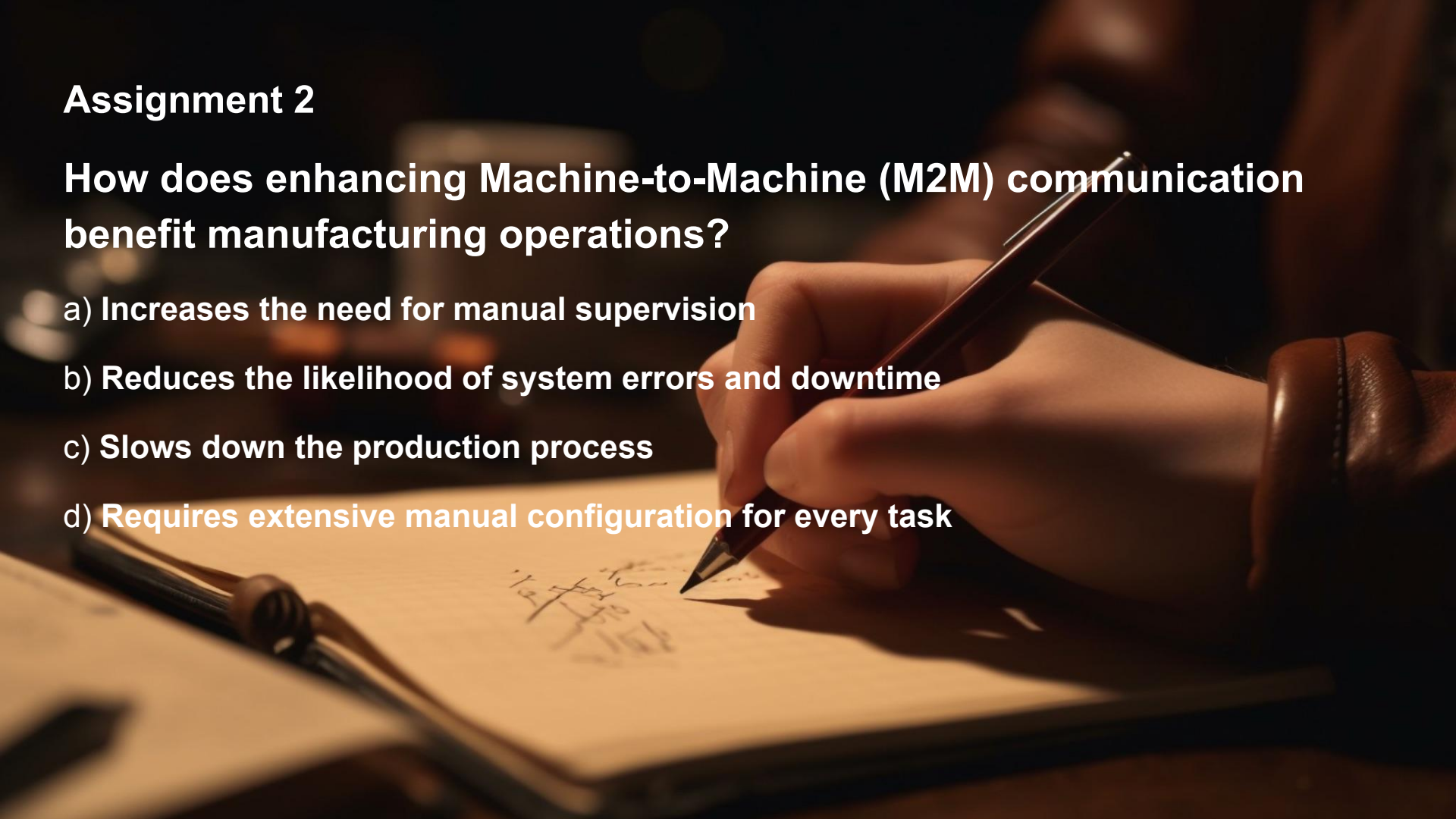
c) **Paper-based tracking systems**

d) **Isolated desktop applications**

Explanation Assignment 1

Correct Answer: b) **Edge devices and gateways**

- **Explanation for Incorrect Options:**
  - **a) Standalone manual workstations:** IIoT focuses on interconnected, automated systems, not manual workstations.
  - **c) Paper-based tracking systems:** IIoT replaces paper-based systems with digital tracking and monitoring.
  - **d) Isolated desktop applications:** IIoT integrates systems and data, moving away from isolated applications.



Assignment 2

How does enhancing Machine-to-Machine (M2M) communication benefit manufacturing operations?

a) **Increases the need for manual supervision**

b) **Reduces the likelihood of system errors and downtime**

c) **Slows down the production process**

d) **Requires extensive manual configuration for every task**

Explanation Assignment 2

Correct Answer: b) **Reduces the likelihood of system errors and downtime**

- **Explanation for Incorrect Options:**
  - **a) Increases the need for manual supervision:** M2M communication reduces the need for manual supervision by automating processes.
  - **c) Slows down the production process:** M2M communication accelerates production by enabling real-time data exchange between machines.
  - **d) Requires extensive manual configuration for every task:** M2M communication is designed to automate tasks, minimizing the need for manual configuration.

Assignment 3

What is one of the main benefits of enhancing data collection through IIoT in manufacturing?

a) **Increased reliance on physical documentation**

b) **Real-time monitoring and predictive maintenance**

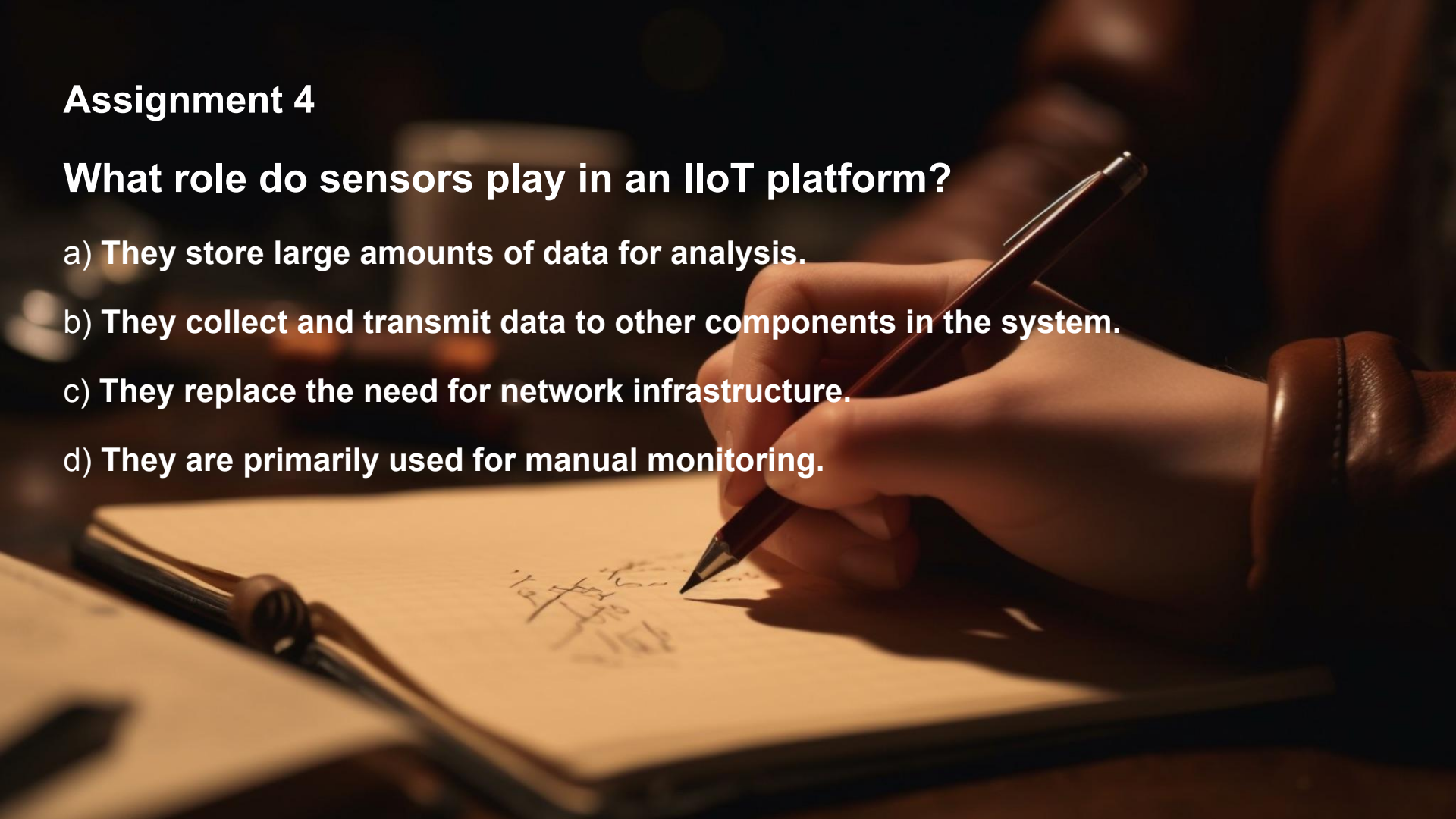
c) **Reduced need for network connectivity**

d) **Decreased system flexibility**

Explanation Assignment 3

Correct Answer: b) **Real-time monitoring and predictive maintenance**

- **Explanation for Incorrect Options:**
  - **a) Increased reliance on physical documentation:** IIoT reduces the need for physical documentation by digitizing data collection.
  - **c) Reduced need for network connectivity:** IIoT relies on strong network connectivity for real-time data collection and analysis.
  - **d) Decreased system flexibility:** IIoT enhances system flexibility by enabling dynamic data-driven decisions.



Assignment 4

What role do sensors play in an IIoT platform?

a) **They store large amounts of data for analysis.**

b) **They collect and transmit data to other components in the system.**

c) **They replace the need for network infrastructure.**

d) **They are primarily used for manual monitoring.**

Explanation Assignment 4

Correct Answer: b) **They collect and transmit data to other components in the system.**

- **Explanation for Incorrect Options:**
  - **a) They store large amounts of data for analysis:** Sensors collect data but do not store it; storage happens in databases or cloud systems.
  - **c) They replace the need for network infrastructure:** Sensors rely on network infrastructure to transmit data.
  - **d) They are primarily used for manual monitoring:** Sensors automate data collection, reducing the need for manual monitoring.

Assignment 5

Which of the following best describes a challenge in enhancing Machine-to-Machine (M2M) communication through IIoT?

a) **Lack of sufficient network bandwidth**

b) **Excessive manual data entry requirements**

c) **Increased system isolation**

d) **Reduction in automated processes**

Explanation Assignment 5

Correct Answer: a) **Lack of sufficient network bandwidth**

- **Explanation for Incorrect Options:**
  - **b) Excessive manual data entry requirements:** M2M communication is designed to minimize manual data entry, not increase it.
  - **c) Increased system isolation:** IIoT and M2M aim to increase connectivity, not isolation.
  - **d) Reduction in automated processes:** M2M communication enhances automation, rather than reducing it.

Learning Objective 3

Benefits & challenges of IoT adoption

Skill Sets to acquire:
Cybersecurity, Data Management, Interoperability, Real-Time Monitoring, Industrial Control System Security, Network Segmentation, Access Control

Core Concepts

- Benefits and challenges of IIoT adoption
- Threat Landscape in Industrial Environments
- Best practices for securing manufacturing systems and data

Benefits and challenges of IIoT adoption

Aspect	Benefits	Challenges	Mitigation Strategies
Cybersecurity	- Enhanced security through continuous monitoring	- Increased attack surface due to more connected devices	- Implement strong encryption, both at rest and in transit
	- Segmentation and control reduces the risk of widespread breaches	- Ensuring up-to-date security patches & firmware on all IoT devices	- Regular firmware updates and network segmentation
		- Data privacy concerns with the large volume of collected data	- Adopt Zero Trust architecture - all devices & users are authenticated & authorized
Data Management	- Enhanced decision-making through real-time data analysis	- Data overload making it difficult to manage and analyze effectively	- Use edge computing to process data locally, reduce the amount sent to central servers
	- Data-driven insights into efficiency, machine performance, energy usage	- Integrating data from various IoT devices and systems	- Implement data filtering to prioritize critical data & adopt scalable cloud-based storage solutions
		- High costs associated with data storage and processing	- Invest in scalable data architecture

Benefits and challenges of IIoT adoption (cont …)

Aspect	Benefits	Challenges	Mitigation Strategies
Interoperability	- Seamless integration of systems across the manufacturing floor	- Compatibility issues between different IoT devices and systems	- Open standards like OPC UA & MQTT ensure compatibility & ease of integration
	- Flexibility to integrate new devices or systems as needed	- Risk of vendor lock-in for proprietary solutions	- Middleware to bridge incompatibilities & ensure vendors prioritize interoperability
		- Lack of industry-wide standards for IoT in manufacturing	- Engage in vendor collaboration to develop integrated solutions, adopt open standards
Real-Time Monitoring	- Immediate insights into production processes and machine performance	- Network latency can hinder real-time data transmission	- Deploy edge computing to process data locally, High-speed networks ie. Ethernet
	- Identifying bottlenecks, reducing downtime for operational efficiency	- Integrating with existing infra - Scalability as devices increases	- Use scalable monitoring solutions that grow with your IoT ecosystem
Predictive Maintenance	- Reduced downtime by predicting and preventing machine failures	- Data accuracy is crucial for reliable predictions	- Start with a pilot project on critical machinery before scaling up
	- Cost savings by performing maintenance only when necessary	- Complexity & cost of implementing predictive maintenance systems	- Advanced analytics & ML for accuracy - Low on-premises investment by Cloud

Threat Landscape in Industrial Environments

Aspect	Threats/Challenges	Examples	Mitigation Strategies
External Cyber Threats	**Advanced Persistent Threats (APTs):**Long-term targeted attacks aimed at stealing data or disrupting operations.	Stuxnet attack on Iran's nuclear facilities.	- Implement multi-layered security (Defense-in-Depth) strategies. - Use firewalls, IDS, and anti-malware solutions.
	Ransomware: Encrypts data and demands ransom for decryption, potentially halting production.	WannaCry attack on Renault, leading to temporary production halts.	- Regularly back up data. - Implement robust incident response plans and user training programs.
	DDoS Attacks: Overwhelm systems with traffic, causing unavailability of systems.	2020 Honda operations disrupted by a suspected DDoS attack.	- Implement DDoS mitigation services and scalable network infrastructure.
Internal Threats	**Insider Threats:** Authorized individuals intentionally or unintentionally cause harm.	Disgruntled employees disabling safety systems or leaking information.	- Implement strict access controls, monitor user activities, and regularly audit access logs.
	Phishing and Social Engineering: Employees are tricked into giving up sensitive information.	Employees unknowingly executing malicious software via phishing emails.	- Conduct regular employee training and phishing simulations. - Use multi-factor authentication (MFA).
Supply Chain Vulnerabilities	**Third-Party Vendor Compromise:**Attackers target less secure vendors to gain access to the manufacturer's systems.	Target data breach in 2013 via an HVAC vendor.	- Enforce strong security policies for third-party vendors and conduct regular security audits.
	Hardware and Software Compromise: Integrating compromised components into systems.	Counterfeit hardware components allowing attackers to control manufacturing systems.	- Implement strict supply chain security and vet all suppliers thoroughly.

Threat Landscape in Industrial Environments

Aspect	Threats/Challenges	Examples	Mitigation Strategies
Legacy Systems and Outdated Technology	**Legacy Systems Vulnerabilities:**Older systems lack modern security features, making them targets.	Industrial Control Systems (ICS) vulnerable to known exploits due to lack of updates.	- Regularly update and patch legacy systems. - Implement compensating controls such as network segmentation.
	Unpatched Systems: Delays in applying patches expose systems to known vulnerabilities.	WannaCry exploited unpatched Windows systems.	- Establish a patch management process to ensure timely updates.
IoT and IIoT Risks	**IoT Device Vulnerabilities:** Limited computing resources make strong security difficult, creating potential entry points.	IoT sensors hacked to provide false data, leading to production errors.	- Use strong encryption, secure boot processes, and regular updates for all IoT devices.
	Data Integrity and Availability Risks: Tampering with IoT data can lead to incorrect decisions or unsafe conditions.	Altering temperature sensor data in a chemical plant, risking unsafe operations.	- Implement real-time monitoring and automated alerts for data anomalies.

Mitigate Cybersecurity Risks in Digital Manufacturing

Implementing a Defense-in-Depth Strategy

- **Description:** A multi-layered approach to security that involves protecting the network, applications, devices, & data
- **Example:** Implement firewalls, intrusion detection systems, & anti-malware solutions at different layers to prevent unauthorized access

Regularly Updating and Patching Systems

- **Description:** Ensure that all systems, including legacy systems, receive regular security patches and updates
- **Example:** Establish a patch management program to identify, test, and deploy patches promptly across all systems

Enhancing Employee Training and Awareness

- **Description:** Train on cybersecurity best practices, including recognizing phishing attempts & understanding role in maintaining security
- **Example:** Conduct regular cybersecurity training sessions and phishing simulations to keep employees vigilant

Strengthening IoT Device Security

- **Description:** Implement strong authentication, encryption, and regular updates for all IoT devices
- **Example:** Secure boot processes & encrypt communication protocols for all IoT devices to prevent unauthorized access & data tampering

Conducting Regular Security Audits and Assessments

- **Description:** Assess security posture of manufacturing environment to identify vulnerabilities & ensure compliance with security policies
- **Example:** Perform penetration testing and vulnerability assessments to identify and mitigate security gaps

Implementing Network Segmentation

- **Description:** Segment the network to isolate critical systems from less secure areas, reducing the risk of widespread attacks
- **Example:** Separate IT and OT networks and use firewalls to control access between different network segments

Securing manufacturing systems - Industrial control System

Best Practice	Description	Implementation
Network Segmentation and Isolation	- Segment ICS networks from corporate IT networks - Isolate critical systems like PLCs and SCADA systems from non-critical systems.	- Use VLANs and firewalls to create network segments. - Implement ACLs to restrict traffic to necessary devices.
Strong Access Control and Authentication	- Implement Role-Based Access Control (RBAC) to limit access to critical ICS components - Use Multi-Factor Authentication (MFA) for accessing ICS networks and systems	- Deploy access management solutions enforcing RBAC and MFA. - Conduct regular audits of user accounts.
Regular Patching and Updates	- Establish a patch management process to keep ICS components up-to-date with security patches - Test patches in a controlled environment before deployment to production systems.	- Use automated tools for patch deployment. - Maintain a test environment for patch testing before deployment.
Intrusion Detection and Prevention (IDPS)	- Deploy IDPS to monitor network traffic and detect unauthorized access or abnormal behavior - Use anomaly detection to identify deviations	- Implement SCADA-specific IDPS solutions. - Configure real-time alerts for suspicious activities.
Defense-in-Depth Strategy	- Adopt a multi-layered security approach to protect ICS from various attack vectors - Ensure redundancy and failover mechanisms for critical ICS components	- Implement firewalls, IDPS, endpoint protection, and physical security controls. - Conduct regular security drills.
Secure Remote Access	- Use VPNs for secure remote access to ICS systems - Monitor all sessions to detect unauthorized activity	- Configure VPNs with high encryption standards. - Monitor and log all remote access sessions.
Incident Response Planning	- Develop an ICS-specific incident response plan with clear communication and recovery steps.	- Establish a dedicated incident response team with expertise in ICS security. - Regularly review and update the plan.

Compliance requirements & industry standards

Standard	Description	Key Requirements for Network Segmentation	Key Requirements for Access Control
NIST Cybersecurity Framework (CSF)	Guidelines cybersecurity risks in critical infrastructure	- Implement segmentation to protect critical assets from threats	- Establish Role-Based Access Control (RBAC) policies
		- Segment networks to limit lateral movement in case of a breach.	- Implement Multi-Factor Authentication (MFA) for critical system access
IEC 62443	Standards for Industrial automation & control systems	- Define zones and conduits to isolate critical systems	- Implement RBAC and enforce strong authentication mechanisms
		- Use firewalls and access control lists (ACLs) to enforce segmentation	- Monitor and log access to critical systems.
ISO/IEC 27001	International standard for information security risks	- Ensure that network segmentation is in place to protect sensitive data	- Access control policies must be documented and enforced across all systems
		- Segmentation should align with the organization’s risk management strategy	- Regularly review and update access control policies to adapt to new threats
PCI DSS (Payment Card Industry Data Security Standard)	A standard for organizations that handle credit card information	- Segmentation of the cardholder data environment (CDE) from other networks is required to reduce PCI scope	- Implement strict access controls, including the principle of least privilege and MFA for sensitive operations
		- Use firewalls to isolate payment processing systems from rest of network	- Access to cardholder data should be restricted based on business need-to-know.

Compliance requirements & industry standards

Standard/Regulation	Description	Key Requirements for Network Segmentation	Key Requirements for Access Control
GDPR (General Data Protection Regulation)	EU regulation-Data protection & privacy for individuals	- Implement network segmentation to protect personal data and limit access to only those who need it.	- Access controls must ensure that personal data is only accessible by authorized personnel.
		- Segment networks to prevent unauthorized access to personal data.	- Implement and regularly audit access control mechanisms to ensure compliance.
HIPAA (Health Insurance Portability and Accountability Act)	U.S. regulation for protecting sensitive patient health information.	- Segmentation of networks to isolate systems containing electronic protected health information (ePHI).	- Implement RBAC and audit access to ePHI regularly.
		- Use firewalls and encryption to protect ePHI during transmission.	- Ensure only authorized personnel can access ePHI, with regular access reviews.
CIS Controls (Center for Internet Security Controls)	A set of best practices for securing IT systems and data against cyber threats.	- Implement network segmentation to limit the attack surface and contain potential breaches.	- Enforce RBAC and use MFA for accessing critical systems and data.
		- Use VLANs, firewalls, and ACLs to create isolated network segments.	- Access control policies should be based on least privilege and regularly reviewed.
CMMC (Cybersecurity Maturity Model Certification)	A standard for assessing cybersecurity maturity for DoD contractors.	- Segmentation to protect Controlled Unclassified Information (CUI) within the contractor's network.	- Implement strict access controls, including MFA, for systems handling CUI.

Norsk Hydro’s response to a ransomware attack

On 19th March 2019, Norsk Hydro, one of the world’s largest aluminum producers, was hit by a severe ransomware attack that crippled its IT systems. Operations in more than 40 countries got affected with production halted across several facilities. Norsk Hydro IT infrastructure supported its production, sales, and logistics operations.

Several of Norsk Hydro’s critical systems were based on legacy platforms that, while robust in their primary functions, lacked modern security features and were difficult to patch or update without significant downtime. Security protocols and practices varied across different global locations, leading to inconsistencies in how systems were protected and monitored. Although Norsk Hydro had basic cybersecurity measures in place, it lacked a comprehensive incident response plan tailored to handle a coordinated, company-wide cyber assault.

The LockerGoga ransomware rapidly encrypted files and spread across the company’s IT network, forcing the company to shut down several production lines and resort to manual operations in some facilities. The attack affected more than 22,000 computers across 170 different sites in 40 countries.

- **Production Halted:** Key production facilities (Qatar, Brazil etc.) were forced to stop or significantly scale back operations
- **Financial Losses:** The attack resulted in estimated losses of $50-70 million, a staggering figure
- **Reputation at Stake:** As a publicly traded company, it faced pressure to swiftly mitigate the impact and restore trust

The pressing need for Norsk Hydro was twofold: First, to restore production and minimize further financial losses, and second, to overhaul its cybersecurity infrastructure to prevent future incidents of this magnitude.

The Attack Vector: The Initial Compromise

Norsk Hydro’s response to a ransomware attack

The LockerGoga ransomware attack was primarily delivered via phishing emails. LockerGoga is known for its stealthy infiltration methods and its ability to cause significant disruption to targeted systems. Here’s how the attack unfolded:

1. **Phishing Email Campaign:**
    - The attack likely began with a spear-phishing campaign, where targeted emails were sent to specific employees within Norsk Hydro. These emails contained either malicious attachments or links to compromised websites.
    - An unsuspecting employee either clicked link or downloaded attachment, which executed a payload.
2. **Initial Malware Execution:**
    - The malicious file began deploying the ransomware across Norsk Hydro’s internal network. The malware initially remained dormant to avoid detection, giving it time to spread across the network and identify key assets to encrypt.
    - LockerGoga’s code was designed to disable security tools, including antivirus, and to change user passwords.
3. **Lateral Movement and Propagation:**
    - The ransomware used various techniques to move - exploiting vulnerabilities in outdated or unpatched systems and using stolen credentials to access additional systems
    - The malware spread rapidly, affecting over 22,000 computers in 170 locations. Critical systems, including those used for production and logistics, were encrypted.
4. **Encryption of Critical Systems:**
    - LockerGoga encrypted a wide range of files on the compromised systems, including critical operational files. The ransomware also displayed a ransom note demanding payment in exchange for the decryption key.
    - However, LockerGoga’s actions suggested a more destructive intent than financial gain, aiming to cause significant disruption. This intent was evident in how thoroughly the systems were disabled.

The exact identity of the attackers remains unclear, but several factors suggest the involvement of a well-organized and sophisticated group. The attack displayed a high level of sophistication, suggesting that the perpetrators had substantial resources and expertise. The use of tailored spear-phishing emails, advanced malware like LockerGoga, and the ability to disable security tools indicate that this was not a random attack, but a targeted and well-planned operation.

Norsk Hydro’s response to a ransomware attack

The Recovery Journey: Steps to Modernize and Secure the Facility

Step 1: Immediate Response and Crisis Management

- **Implementation:** Norsk Hydro’s initial response focused on isolating the infected systems to prevent further spread of the ransomware. The IT team, working alongside external cybersecurity experts, quickly began efforts to contain the attack.
- **Outcome:** Despite the disruption, Norsk Hydro made the decision not to pay the ransom, instead opting to rely on backups and manual operations while systems were restored. This decision was driven by a commitment to not incentivize criminal activities and to maintain the integrity of its operations.

Step 2: Restoring Operations

- **Implementation:** With the support of cybersecurity experts from Microsoft and other partners, Norsk Hydro rebuilt servers, restoring data from backups, and gradually bringing production systems back online.
- **Outcome:** Production gradually resumed over the following weeks, with Norsk Hydro prioritizing critical operations and customer commitments. The company managed to fully restore operations without paying the ransom, a decision that was praised by cybersecurity professionals.

Step 3: Cybersecurity Modernization

- **Upgrading Legacy Systems:** The company accelerated its plans to replace legacy systems with modern, secure platforms that could be more easily updated and patched.
- **Centralized Security Management:** Norsk Hydro centralized its cybersecurity operations, implementing a unified security operations center (SOC) that provided real-time monitoring and rapid response capabilities across all global sites.
- **Enhanced Incident Response Plan:** including detailed procedures for responding to various types of cyber threats, as well as regular drills to ensure preparedness.
- **Adoption of Zero Trust Architecture:** Every user, device, and application was required to be authenticated, authorized, and continuously validated before access to critical systems was granted.

Norsk Hydro’s response to a ransomware attack

Recognizing that human error often plays a role in successful cyberattacks, Norsk Hydro launched a comprehensive cybersecurity training program for all employees. This program emphasized the importance of vigilance, proper handling of suspicious emails, and adherence to security protocols.

Norsk Hydro strengthened its partnerships with leading cybersecurity firms, including Microsoft and PwC, to ensure continuous support and access to the latest threat intelligence and security technologies.

Levels Achieved After the Exercise

- **System Uptime and Reliability:** The modernization of IT systems and the implementation of a Zero Trust architecture led to a 40% reduction in system vulnerabilities, enhancing the overall reliability of Norsk Hydro’s operations.
- **Incident Response Time:** With the establishment of a centralized SOC and a robust incident response plan, Norsk Hydro reduced its incident response time by 50%, allowing for quicker detection and mitigation of potential threats.
- **Employee Cybersecurity Awareness:** The company’s training programs resulted in a marked decrease in phishing-related incidents, with reported cases dropping by 30% within the first year.

Competition and market response

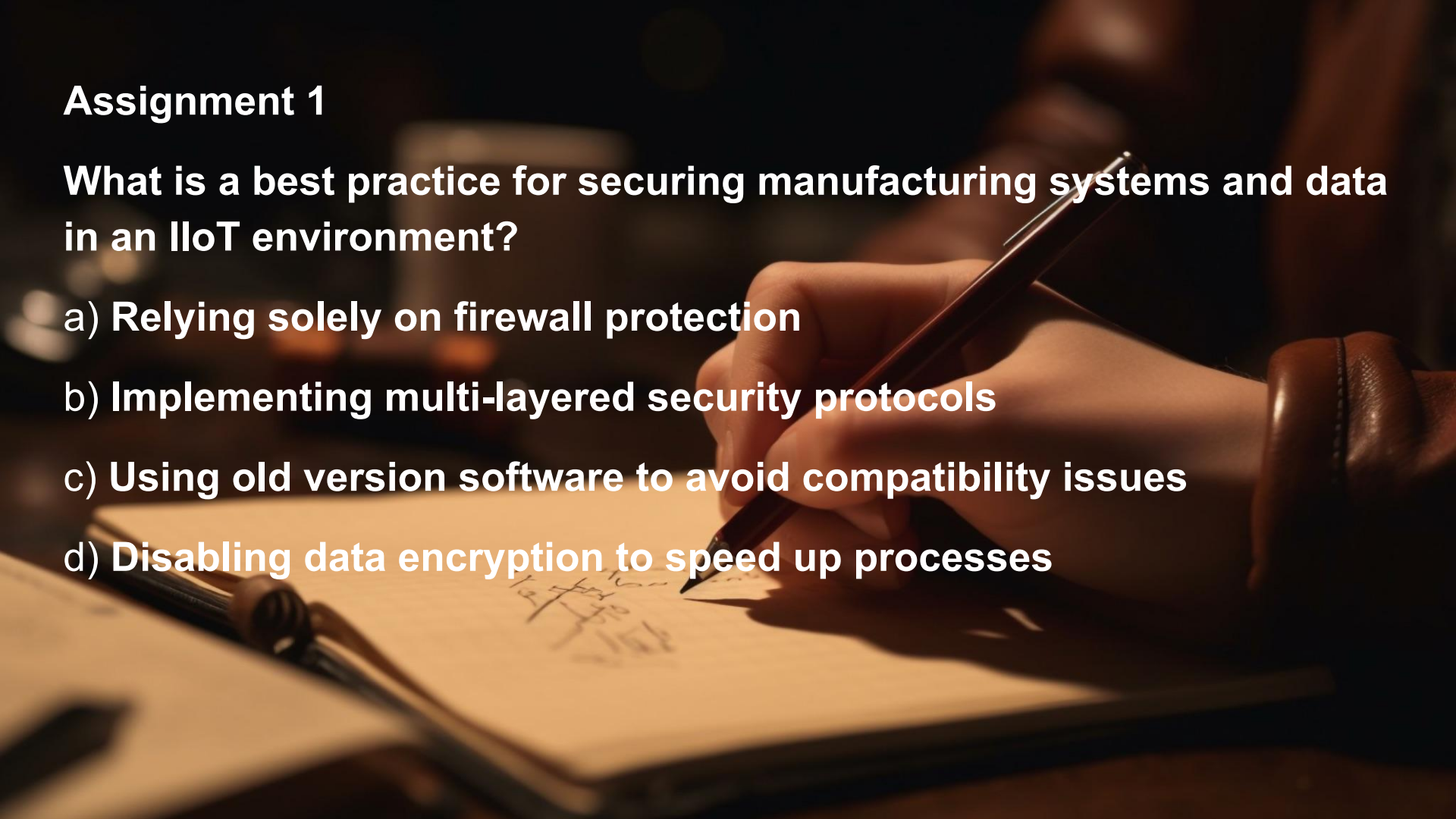
Norsk Hydro’s decision to refuse the ransom and rebuild its systems from backups, while challenging, was accomplished within a few weeks. This is notably faster than many organizations of similar size, which can take months to fully recover from such attacks. Despite the initial financial losses, it avoided ransom payments and potential follow-up attacks.

The incident highlighted the growing threat of ransomware in the industrial sector, prompting companies across the aluminum and broader manufacturing industries to invest heavily in cybersecurity. Competitors such as Alcoa and Rio Tinto increased their cybersecurity budgets and accelerated the adoption of modern security practices, such as Zero Trust and centralized monitoring.

Common follow-up questions

1. What are the key benefits of adopting Industrial IoT (IIoT) in manufacturing, and how do they translate to tangible improvements in operations?
2. What are the primary security challenges associated with IIoT adoption in industrial environments?
3. How can manufacturers balance the benefits of IIoT with the potential risks, particularly in terms of data security and system integrity?
4. What are some common threat vectors in industrial environments that are exacerbated by IIoT adoption?
5. What best practices should be followed to secure manufacturing systems and data when implementing IIoT solutions?

Assessment



Assignment 1

What is a best practice for securing manufacturing systems and data in an IIoT environment?

a) **Relying solely on firewall protection**

b) **Implementing multi-layered security protocols**

c) **Using old version software to avoid compatibility issues**

d) **Disabling data encryption to speed up processes**

Explanation Assignment 1

Correct Answer: b) **Implementing multi-layered security protocols**

- **Explanation for Incorrect Options:**
  - **a) Relying solely on firewall protection:** Firewalls are important, but a comprehensive security strategy requires more than just firewalls.
  - **c) Using old version software to avoid compatibility issues:** Outdated software can have unpatched vulnerabilities, increasing security risks.
  - **d) Disabling data encryption to speed up processes:** Disabling encryption exposes data to significant risks.

Assignment 2

Which benefit does IIoT bring to the operational efficiency of manufacturing systems?

a) **Introduction of manual monitoring processes**

b) **Increased downtime due to system complexity**

c) **Real-time monitoring and control of production processes**

d) **Reduction in automated quality control measures**

Explanation Assignment 2

Correct Answer: c) **Real-time monitoring and control of production processes**

- **Explanation for Incorrect Options:**
  - **a) Introduction of manual monitoring processes:** IIoT automates monitoring, reducing the need for manual processes.
  - **b) Increased downtime due to system complexity:** While complexity may increase, IIoT is designed to reduce downtime through automation and real-time insights.
  - **d) Reduction in automated quality control measures:** IIoT enhances quality control by enabling real-time monitoring and adjustments.

Assignment 3

What is a potential downside of IIoT adoption in terms of data security?

a) **Improved data accuracy and availability**

b) **Increased risk of data breaches**

c) **Decreased need for regular security audits**

d) **Enhanced ability to secure legacy systems**

Explanation Assignment 3

Correct Answer: b) **Increased risk of data breaches**

- **Explanation for Incorrect Options:**
  - **a) Improved data accuracy and availability:** While data accuracy and availability improve, the security risks also increase.
  - **c) Decreased need for regular security audits:** IIoT adoption increases the need for frequent security audits to address new vulnerabilities.
  - **d) Enhanced ability to secure legacy systems:** Securing legacy systems often becomes more challenging with IIoT adoption due to compatibility issues.

Assignment 4

Which of the following is a common threat vector in IIoT-enabled industrial environments?

a) **Phishing attacks targeting factory workers**

b) **Unpatched software vulnerabilities in connected devices**

c) **Physical theft of machinery**

d) **Lack of training for manual assembly tasks**

Explanation Assignment 4

Correct Answer: b) **Unpatched software vulnerabilities in connected devices**

- **Explanation for Incorrect Options:**
  - **a) Phishing attacks targeting factory workers:** While phishing is a general threat, unpatched software vulnerabilities specific to IIoT are more critical.
  - **c) Physical theft of machinery:** Physical threats exist, but the question focuses on IIoT-related risks.
  - **d) Lack of training for manual assembly tasks:** This is unrelated to IIoT-specific threats.

Assignment 5

What is a best practice for securing IIoT devices in a manufacturing setting?

- a) **Disabling software updates to prevent system changes**
- b) **Using strong, unique passwords for each device**
- c) **Avoiding network segmentation to maintain system simplicity**
- d) **Relying on default settings for all devices**

Explanation Assignment 5

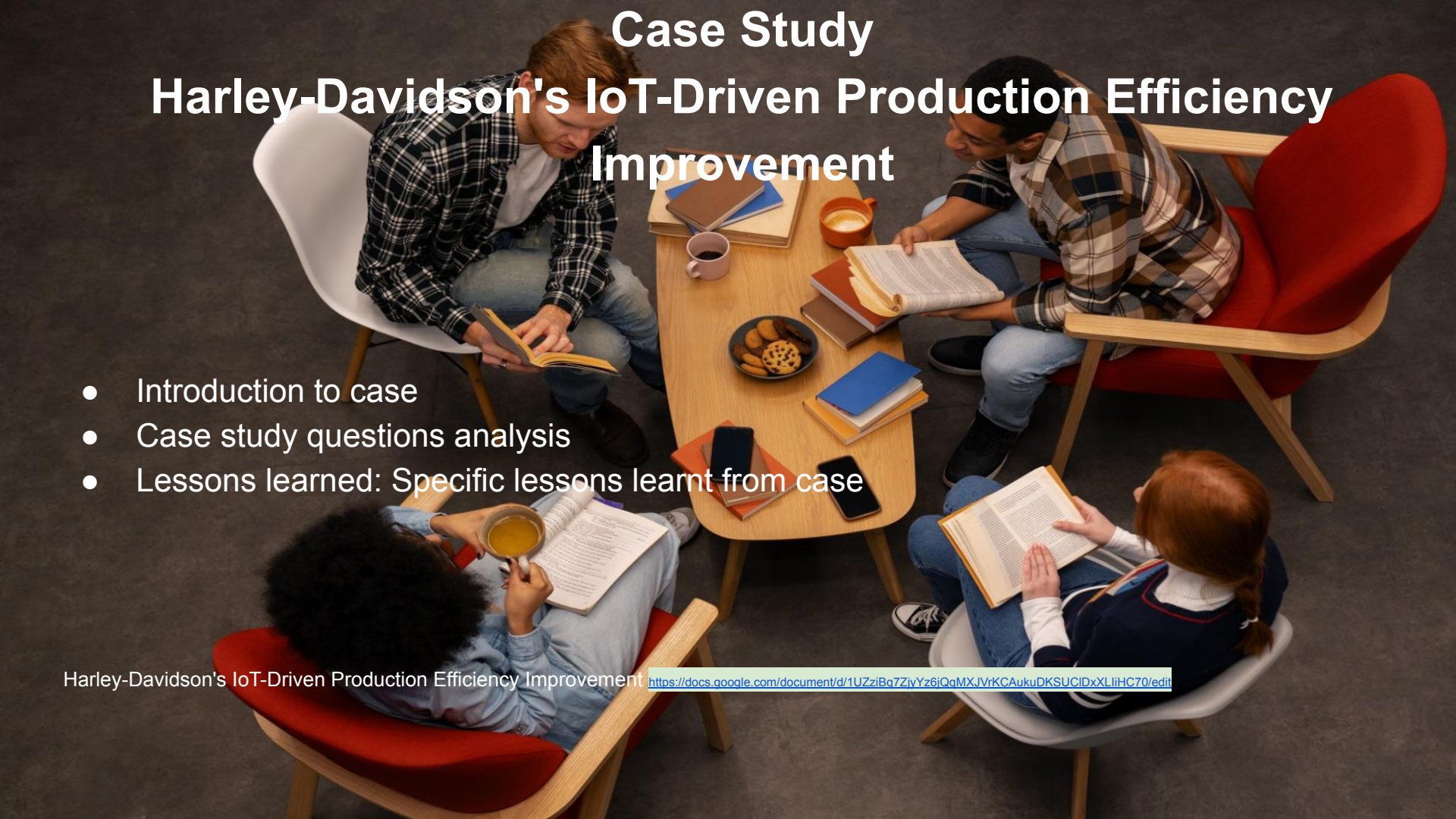
Correct Answer: b) **Using strong, unique passwords for each device**

- **Explanation for Incorrect Options:**
  - **a) Disabling software updates to prevent system changes:** Updates are crucial for patching vulnerabilities and should not be disabled.
  - **c) Avoiding network segmentation to maintain system simplicity:** Network segmentation is a best practice to contain potential breaches.
  - **d) Relying on default settings for all devices:** Default settings are often less secure; customizing settings enhances security.

ZEN LEARN

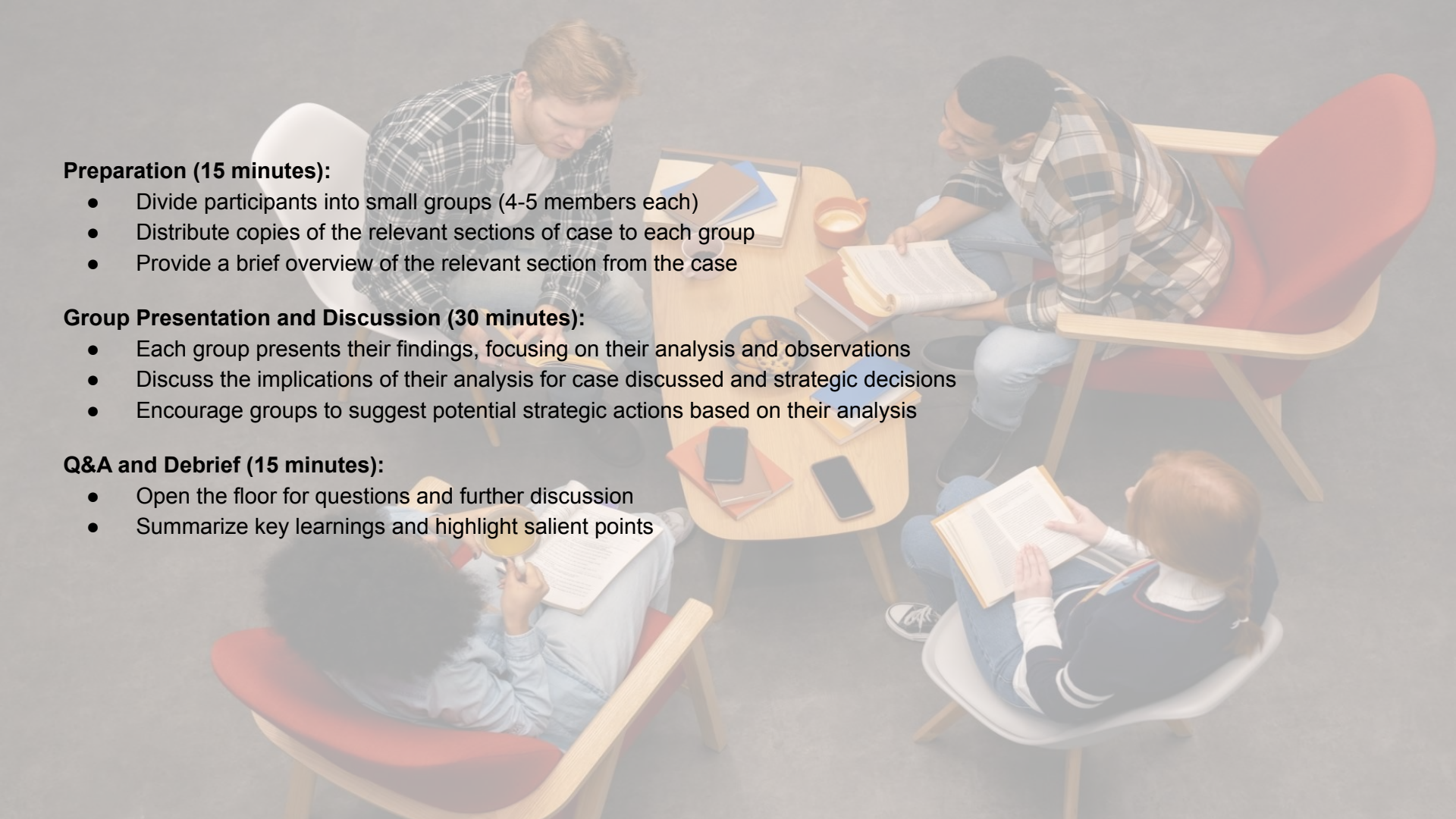
Case Study

Case Study
Harley-Davidson's IoT-Driven Production Efficiency Improvement



- Introduction to case
- Case study questions analysis
- Lessons learned: Specific lessons learnt from case

Harley-Davidson's IoT-Driven Production Efficiency Improvement https://docs.google.com/document/d/1UZziBq7ZjyYz6jQqMXJVrKCAukuDKSUClDxXLIiHC70/edit



Preparation (15 minutes):

- Divide participants into small groups (4-5 members each)
- Distribute copies of the relevant sections of case to each group
- Provide a brief overview of the relevant section from the case

Group Presentation and Discussion (30 minutes):

- Each group presents their findings, focusing on their analysis and observations
- Discuss the implications of their analysis for case discussed and strategic decisions
- Encourage groups to suggest potential strategic actions based on their analysis

Q&A and Debrief (15 minutes):

- Open the floor for questions and further discussion
- Summarize key learnings and highlight salient points

Interactive Exercise

Role-Playing Exercise (20 minutes)

Scenario: In this role-playing exercise, participants will simulate a board meeting where they must decide on the next steps for Harley-Davidson’s digital transformation.

Roles: Assign participants different roles, such as the CEO, CTO, Head of Operations, and Chief Digital Officer. Provide each role with specific objectives or concerns.

Task: The "board" must discuss and decide on the following:

- Whether to expand IoT initiatives to other plants or focus on optimizing the existing implementation.
- Which emerging technologies (e.g., AI, blockchain, AR/VR) should be considered for future adoption.
- How to balance the investment in technology with workforce development and training.

Interactive Exercise

Smart Factory Simulation: Designing an IoT-Enabled Factory

Objective: Participants will learn the fundamentals of implementing IoT in manufacturing by designing and simulating an IoT-enabled production line. This exercise will help them understand how IoT devices can be integrated into manufacturing processes to improve efficiency, monitor performance, and enable predictive maintenance. **Duration:** 90 minutes

Materials Needed:

- Laptops or tablets with internet access
- Virtual whiteboard or flip charts
- IoT simulation software or platform (e.g., ThingWorx, Ignition, or a simplified simulation tool)
- Pre-defined case study materials (including factory layout, types of machines, current challenges)
- Post-it notes, markers, and pens (if using physical materials)

Group Size: 4-6 participants per group

Participant Brief:
Imagine you are a consultant hired by a mid-sized motorcycle manufacturer that wants to replicate Harley-Davidson's success by implementing IoT in its production process.

Each group will develop a high-level IoT implementation plan for the manufacturer. The plan should include:

- Key areas of the production process to target with IoT.
- Recommended IoT technologies and digital tools.
- A phased timeline for implementation.
- Expected outcomes and how they will be measured.

Presentation: Each group will present their IoT implementation plan, explaining the rationale behind their choices and how they expect the manufacturer to benefit from the IoT integration.

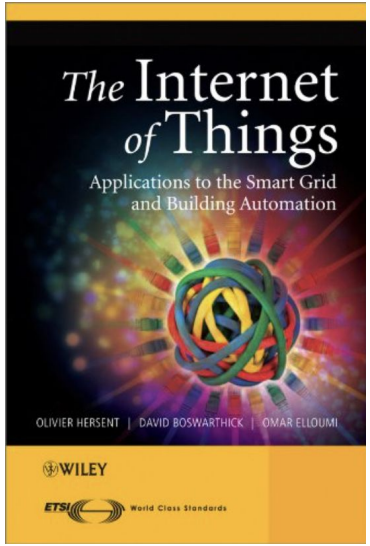
Assignment questions

- Question 1
- Question 2
- Question 3

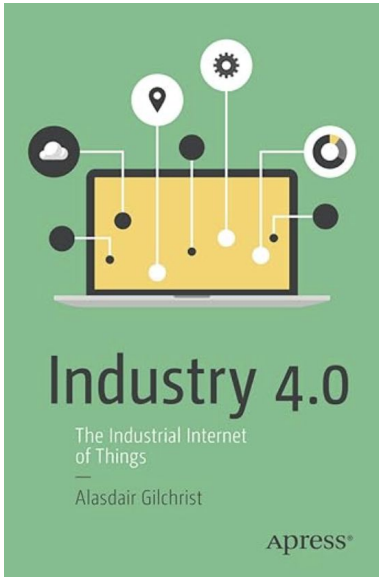
Questions & Further Reading

Q&A
Feedback

Recommended Books

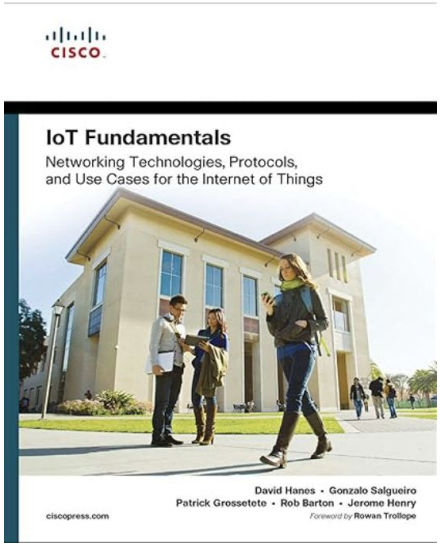


The Internet of Things: Key Applications and Protocols
Olivier Hersent

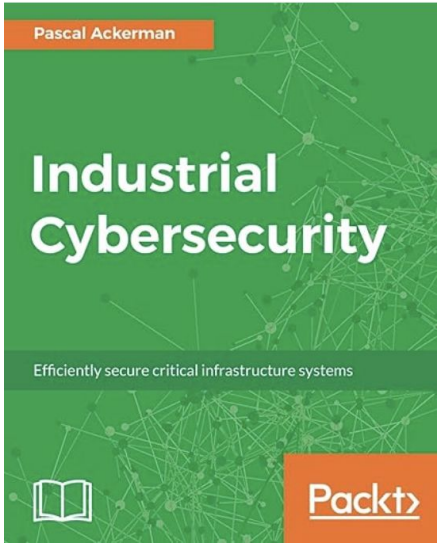


Industry 4.0: The Industrial Internet of Things
Alasdair Gilchrist

Recommended Books



[IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things
David Hanes]

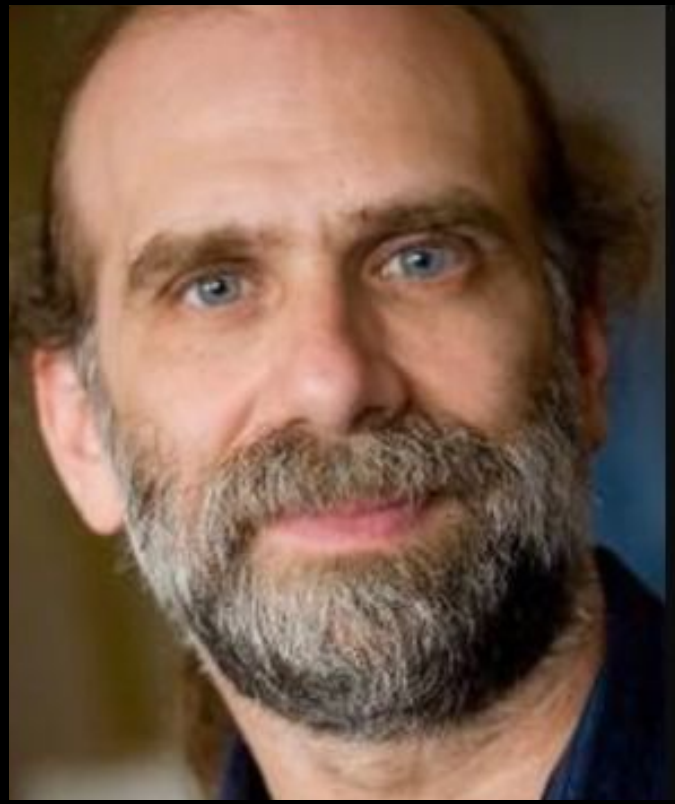


[Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems
Pascal Ackerman]

यत्रोपरमते चित्तं निरुद्धं योगसेवया ।
यत्र चैवात्मनात्मानं पश्यन्नात्मनि तुष्यति ॥

In the still mind, in the depths of meditation, the Self reveals itself

Bhagavad Gita
6:20



Security is a process, not a product.

— Bruce Schneier —


ZEN
LEARN