

*ASSESSMENT OF IIOT SENSOR SECURITY  
VULNERABILITIES IN AI-DRIVEN DIGITAL  
MANUFACTURING*

Presenter: Dr Sachin Sen

Affiliation: Unitec Institute of Technology

→ Conference: ITP Symposium – 2025, 01 December 2025.

## *INTRODUCTION*

- AI-driven digital manufacturing transforms industrial operations through automation and intelligent decision-making.
- IIoT sensors supply the real-time data required for these AI models.
- Increased reliance on sensors expands the cybersecurity threat surface.

## *MOTIVATION*

- Sensor-level compromises can corrupt AI model outputs.
- Small data manipulation leads to large operational consequences.
- Protecting IIoT sensors is critical for maintaining industrial resilience.



## *ROLE OF IIOT SENSORS IN AI MANUFACTURING*

- Collect environmental, operational, and machine status data.
- Enable predictive maintenance, quality control, and autonomous adjustments.
- Form the foundation for AI analytics and decision-making.

## *CYBERSECURITY CHALLENGES*

- Sensors often operate in exposed or distributed environments.
- Limited computational resources reduce built-in security.
- Heterogeneous sensor ecosystems complicate standardised protection.



## *KEY SENSOR-LEVEL VULNERABILITIES*

- **Spoofing:** Injection of false sensor data.
- **Tampering:** Physical or digital modification of sensor output.
- **Denial-of-Service (DoS):** Blocking sensor communication or flooding the network.
- **Data Leakage:** Unauthorised access or exposure of sensor data.

## *CONSEQUENCES OF SENSOR COMPROMISE*

- Corrupts AI model predictions and control decisions.
- Causes production disruptions and downtime.
- Impacts product quality and consistency.
- Potential safety hazards for workers and equipment.



## *RESEARCH OBJECTIVES*

- Systematically assess IIoT sensor vulnerabilities in AI-enabled manufacturing.
- Apply the Common Vulnerability Scoring System (CVSS) for quantitative risk evaluation.
- Align findings with industrial cybersecurity standards (NIST).
- Prioritise vulnerabilities based on severity and operational impact.

## *OVERVIEW OF THE METHODOLOGY*

- Identify key IIoT sensor threat scenarios.
- Perform CVSS-based scoring for each scenario.
- Map findings to NIST industrial cybersecurity controls.
- Evaluate the impact of sensor data corruption on AI-model reliability.



## *APPLICATION OF CVSS*

- Measures exploitability, impact, and severity on a 0–10 scale.
- Base metrics evaluate inherent vulnerability attributes.
- Environmental metrics consider the manufacturing context.
- Enables prioritisation of high-risk vulnerabilities.

## *AI VULNERABILITY TO SENSOR ATTACKS*

- AI models depend on accurate, trustworthy data.
- Data poisoning or manipulation leads to:
  - Incorrect predictions
  - Faulty control signals
  - Misaligned processes
- Creates cascading effects across production lines.



*CASCADING RISK  
IN  
SMART MANUFACTURING*

- One corrupted sensor → faulty AI inference → incorrect machine behaviour.
- Multi-sensor attacks can destabilise entire production systems.
- The complexity of AI pipelines magnifies small errors.

## *MITIGATION STRATEGIES*

- Secure Authentication: Verify sensor identity and communication integrity.
- Real-Time Anomaly Detection: Detect abnormal sensor behaviour using ML.
- Sensor Redundancy: Cross-check data with parallel sensing units.
- Data Validation: Filter and verify data before feeding AI algorithms



## *INTEGRATION WITH INDUSTRIAL STANDARDS*

- Aligns with NIST SP 800-82 and NIST CSF guidelines.
- Supports risk prioritisation, continuous monitoring, and incident response.
- Provides structured pathways for improving ICS/IIoT cyber-resilience.

## *KEY FINDINGS*

- IIoT sensors represent highly vulnerable cyber-physical nodes.
- CVSS scoring provides objective prioritisation of sensor risks.
- AI-driven systems amplify the consequences of sensor attacks.
- A sensor-centric cybersecurity perspective strengthens industrial resilience.



## *CONTRIBUTIONS*

- Introduces a systematic, quantitative approach to evaluating sensor vulnerabilities.
- Highlights the interdependency between sensor integrity and AI model reliability.
- Provides practical mitigation and protection strategies for manufacturers.

## *CONCLUSION*

- Sensor security is fundamental to trustworthy AI in digital manufacturing.
- Proactive vulnerability assessment reduces risks and operational disruptions.
- Strengthening sensor cybersecurity enhances the resilience of future smart factories.



*THANK YOU*

*Q&A*

Now, time for Questions and Discussions.