Cybersecure Mechatronic and Robotic Systems

Advanced Mechatronics, Robotics, and Cybersecurity Integration for Future Technologies

---

Introduction:

Cybersecure Mechatronic and Robotic Systems is a hands-on course focused on the practical cybersecurity challenges of modern robotics, mechatronics, and IoT systems. Unlike traditional computer science or electrical engineering courses that emphasize programming or debugging, this course centers on system-level integration and protection of connected, intelligent machines. Students will explore secure digital twins, quantum-resistant cryptography, federated learning, and AI-enhanced control while examining how these technologies apply to real-world sectors such as autonomous vehicles, smart healthcare, and industrial automation. Designed for students and professionals with a background in mechatronics, the course requires no additional prerequisites and offers an accessible, interdisciplinary approach that builds directly on existing engineering foundations.

Section 1: Advanced Mechatronics Systems and Cybersecurity Integration

Topics to Cover:

- Foundation: The Intelligent, Real-Time Edge
  - Evolution of Mechatronics: From Mechanical Systems to Intelligent Automation
  - Embedded Systems and IoT (Internet of Things) in Mechatronics
  - Real-Time Systems and Control Architectures
- Verification and Vulnerability
  - Hardware-in-the-Loop (HIL) Simulation and Testing
  - Cybersecurity Threats in Mechatronic Systems: Threat Models and Risk Assessment
- Defense Architecture: Autonomy and Integrity
  - Digital Twins for Secure Mechatronic Systems
  - Secure Communication Protocols for Cyber-Physical Systems (CPS)
  - AI Integration into Mechatronics: Edge AI and Federated Learning Security
  - Blockchain for Distributed Mechatronic System Security

Section 2: Robotics Science, Emerging Research Frontiers, and Cybersecurity Challenges

Topics to Cover:

- Foundations: Motion, Intelligence, and Integration of cyber security
    - Soft Robotics and Bio-Inspired Robotics
    - Robot Operating System (ROS 2) and Cybersecurity Layers
- Collective Behaviour and Human Interaction
    - Multi-Agent Systems and Swarm Robotics
- The Battle for Robotic Intelligence and Trust
    - Trusted AI for Robotic Systems (Ethics in AI)
- Network Resilience and Critical Applications
    - Robotics and 5G/6G Communication Security
    - Defense and Critical Infrastructure Robotics: Cyber Warfare Preparedness

---

Section 3: Cybersecurity, Robotics, and Emerging Consumer Applications

Topics to Cover:

- Application Domains and Unique Cyber Threats
    - Smart Home Robotics: Privacy, Data Protection, and Intrusion Detection
    - Service Robotics (Healthcare, Elderly Care, Delivery) and Cyber Risk Management
    - Consumer Drones and Autonomous Vehicles: Security and Regulation
    - Industrial IoT (IIoT) and Smart Factories: Robotics + Cybersecurity Challenges
    - Wearable Robotics and Exoskeletons: Cybersecurity for Human Augmentation
    - Virtual Reality (VR) and Augmented Reality (AR) Robotics Systems Security
- Advanced Security Architecture
    - Blockchain and Tokenization in Consumer Robotic Networks
- Ethics, Governance, and Legal Compliance
    - AI Ethics and Governance in Consumer Robotics
    - Legal and Regulatory Landscape: GDPR, CCPA, and Beyond
- Commercialization and future Outlook
    - Startups and Innovations in Consumer Robotics: From Idea to Market

---

Introduction of the Cutting-Edge Tools and Technologies to Integrate

- ROS 2 (Robotics Middleware)
- Gazebo/Isaac Sim (Robotics simulation)
- Nvidia Deep Learning frameworks for robotics (Isaac SDK, Jetson platforms)

- Cybersecurity frameworks (NIST Cybersecurity Framework, MITRE ATT&CK for ICS)
- Blockchain platforms (Hyperledger Fabric for robotics networks)
- Cloud Robotics platforms (AWS RoboMaker, Azure IoT Hub with Robotics SDKs)

---

1. Week-by-Week Syllabus (13 Weeks)

Week 1 - Advanced Mechatronics and Cybersecurity
Week 2 - Modern Mechatronics and Embedded Architectures
Week 3 - Fundamentals for Cyber-Physical Systems
Week 4 - Digital Twins and Secure Real-Time Simulations
Week 5 - Securing Agentic IoT
Week 6 - Securing the Agentic Frontier
Week 7 - Mid-Term Project Proposal Presentations
Week 8 - ROS 2 and Middleware Security
Week 9 - Soft Swarm Robotics New Frontiers
Week 10 - Critical Infrastructure and 5-6G Resilience
Week 11- Legal, Ethical, and Societal Challenges
Week 12 - Future Trends and Wrap-Up
Week 13 - Final Capstone Project Presentations

---

2. Key References (Books, Papers, Standards)

Core Books:

- **"Cyber-Physical Systems: Foundations, Principles and Applications"** by Raj Rajkumar et al.
- **"Practical Industrial Internet of Things Security"** by Sravani Bhattacharjee

Academic Papers (Examples for Seminar Readings):

- *"Secure and Resilient Cyber-Physical Systems: Architectures and Design Principles"*, IEEE Transactions on CPS
- *"Security Challenges for Robot Operating Systems"*, International Journal of Advanced Robotic Systems
- *"Adversarial Attacks Against Deep Learning-Based Robotic Vision Systems"*, IEEE Access

Important Standards:

- **NIST Cybersecurity Framework 1.1**
- **MITRE ATT&CK for ICS (Industrial Control Systems)**
- **ISO/IEC 27001 (Information Security Management Systems)**
- **ROS Enhancement Proposals (REPs) regarding Security (e.g., REP-2004)**

---

3. Suggested Research Project Ideas

Area	Project Title	Description
Mechatronics + IoT Security	**Design of a Secure IoT-enabled Mechatronic System**	Concept Study, penetration and analysis
Robotics + Secure Physical AI	**Resilient SLAM Algorithms against Adversarial Attacks**	Concept Study, penetration and analysis
Consumer Robotics Security	**Privacy-Preserving Control of Consumer Drones**	Concept Study, penetration and analysis
Cybersecurity + Blockchain	**Blockchain-based Identity Management for Robotic Swarms**	Concept Study, penetration and analysis
Critical Infrastructure and Robotic Security	**Cyber Attack Detection in Industrial Robot Networks**	Concept Study, penetration and analysis
IoT Digital Twins	**Secure Digital Twin for Predictive Maintenance**	Concept Study, penetration and analysis
Edge AI	**Secure Federated Learning in Mobile Robotics**	Concept Study, penetration and analysis
Ethics	**Bias and Fairness Testing in AI-based Robotic Decisions**	Create an audit framework for ethical decision-making in robots

---

✅ 2. Evaluation Breakdown

Component	Weight	Description
Mid-Term Project Proposal + Presentation	20%	Proposal of a novel problem and secure solution
Final Capstone Project	40%	Design + Implementation + Defense
Real word innovation and research idea	20%	ROS2, digital twins, secure firmware, etc.
Final Written Report (Research Paper Style)	10%	IEEE format submission

Component	Weight	Description
Class Participation & Peer Review	10%	Class engagement, discussions, and feedback

---

✅ 3. Visual Roadmap: Integrated Technology Domains