



UNIVERSITY OF
TORONTO

MIE1810: Cybersecurity in Autonomous and Robotic Systems

Graduate Course Syllabus

University of Toronto | Faculty of Applied Science and Engineering | Department of Mechanical and Industrial Engineering

Course Code: MIE1810 | **FCE Weight:** 0.5 | **Course Type:** Regular

Delivery: In person | **Contact Hours:** 2 lecture hours per week | **Prerequisite:** Consult with instructor

1.1 Course Overview

This graduate course explores the integration of mechatronics, robotics, autonomous systems, and cybersecurity, with emphasis on real-world, system-level security challenges rather than traditional programming alone. Students examine secure AI-enhanced control systems, embedded and cyber-physical system vulnerabilities, digital twins, threat modeling, secure communication, federated learning, quantum-resistant cryptography, and cyber-resilience validation. The course is designed for graduate students in research and professional master's streams who are interested in designing secure robotic, mechatronic, autonomous, and cyber-physical systems for applications such as autonomous vehicles, smart healthcare, industrial automation, and connected infrastructure.

1.2 Course Description

This course examines cybersecurity as a core design requirement for autonomous, robotic, mechatronic, and cyber-physical systems. Through technical readings, applied case studies, project-based work, and class discussion, students will develop the ability to identify system vulnerabilities, assess cyber-physical risks, and propose secure, resilient design strategies for real-world engineering applications.

1.3 Learning Outcomes

- Explain major cybersecurity challenges affecting autonomous, robotic, mechatronic, and cyber-physical systems.
- Identify vulnerabilities in embedded systems, sensors, actuators, controllers, communications, and AI-enabled control architectures.

- Apply threat modeling and risk assessment methods to cyber-physical engineering systems.
- Evaluate secure communication, digital twin, edge security, federated learning, blockchain, and resilience validation approaches.
- Design and defend a technically grounded security solution for a robotic, autonomous, or cyber-physical system.

1.4 Weekly Course Topics

Week	Topic
1	<i>Physical AI & Autonomous Systems Security, Physical AI, embodied intelligence, autonomous robotics, Edge AI, cyber-physical systems, and the evolving cyber threat landscape</i>
2	<i>Cyber Architecture of AI-Native Autonomous Systems, sensors, actuators, controllers, ROS 2/DDS, edge compute, AI models, networks, cloud services, digital twins, and physical/digital interfaces</i>
3	<i>Cyber Architecture Modeling & Attack-Surface Discovery, network and system architecture modeling, assets, interfaces, data flows, trust boundaries, zones/conduits, attack surfaces, and machine-readable/interoperable architecture models for cyber analytics</i>
4	<i>Attack Paths, Threat Modeling & Cyber Risk Assessment, attack graphs, STRIDE, attack trees, MITRE ATT&CK/ICS, NIST CSF/RMF, risk characterization, architecture-driven vulnerability and security-gap identification</i>
5	<i>Edge AI & AI Supply-Chain Security, edge inference, AI accelerators, containers, APIs, model deployment, OTA updates, SBOM/AIBOM, provenance, dependencies, model integrity, and supply-chain compromise</i>
6	<i>Adversarial AI & Physical AI Attacks, sensor spoofing, adversarial perception, data/model poisoning, backdoors, model theft, multimodal attacks, and perception-to-decision-to-action attack pathways</i>
7	<i>Agentic AI & Autonomous Decision Security, autonomous agents, tool/API abuse, context and goal manipulation, excessive autonomy, authority boundaries, human oversight, runtime guardrails, and secure machine decision-making</i>

Week	Topic
8	<i>Zero Trust, Identity & Secure Communications, device/workload identity, PKI, authentication, authorization, segmentation, secure ROS 2/DDS, edge-cloud communications, command-and-control security, and Zero Trust architecture</i>
9	<i>Digital Twins, HIL & Cybersecurity Validation, security-aware digital twins, hardware-in-the-loop, cyber ranges, network emulation, attack/fault injection, anomaly detection, penetration testing concepts, and validation of architectural defenses</i>
10	<i>Cyber Resilience, Safety & Mission Assurance, cyber-to-physical consequences, safety-security interaction, graceful degradation, fail-safe/fail-operational design, recovery, resilience engineering, and mission-critical autonomy</i>
11	<i>Post-Quantum & Distributed Autonomous Systems Security, post-quantum cryptography, crypto-agility, constrained edge platforms, swarm robotics, multi-agent systems, collaborative autonomy, and next-generation distributed Physical AI</i>
12	<i>Cyber Architecture Design Review & Capstone, complete architecture assessment: assets → trust boundaries → attack surfaces → attack paths → risks → security gaps → controls → secure redesign → validation → residual risk</i>

2 Assessment and Evaluation

Assessment	Weight	Description
Individual Mid-Term Project Proposal and Presentation	15%	Proposal of a novel system security problem and a secure solution approach.
Weekly Seminar Critiques	15%	Analytical reviews of current research papers and technical literature.
Real-World Innovation and Research Idea	20%	Applied concept development involving ROS 2, digital twins, secure firmware, cyber-resilience, or related technologies.
Final Capstone Project	30%	Design, implementation, and technical defense of a secure robotic, autonomous, or cyber-physical system concept.

Final Written Report	10%	Research-paper-style written submission in a technical format.
Participation and Peer Review	10%	Class engagement, discussion contributions, and constructive feedback to peers.

3 Capstone Project Expectations

The final capstone may be framed as an industry-style system security deliverable. Possible formats include a secure robotics architecture review, a threat model and mitigation plan for a cyber-physical product, a secure digital-twin deployment with attack-surface analysis, or a cyber-resilience validation report using hardware-in-the-loop simulation. Expected deliverables may include a system architecture diagram, threat model, risk mitigation justification, implementation evidence where appropriate, and a technical defense presentation.

4 Required Textbook

Houbing Song, Danda B. Rawat, Sabina Jeschke, and Christian Brecher, *Cyber-Physical Systems Security: Foundations and Challenges*, Wiley-IEEE Press, ISBN 9781119226045.