GRADUATE CERTIFICATE IN SYSTEMS SECURITY

Students will learn how to understand, implement, measure, validate and verify security properties of complex systems. Content will cover common threats, vulnerabilities, processes, policies and methods for security such as: threat analysis and risk assessment, networking, physical security, information system security, and operational technology security. Students gain hands-on experience designing, implementing, and assessing the security postures of cyber-physical systems through a rigorous foundation in the best practices for information security while overcoming the challenges associated with the limiting environment found in operational technology.

The Certificate combines cybersecurity for systems engineers, networking concepts as seen in personal computers (TCP/IP), Controller Area Networks (CAN bus) as seen in vehicles and industrial systems, manufacturing, supply chains, system modeling, policy development, and protections systems for confidentiality, integrity, and system availability as primary goals. Completion of the certificate allows students to bring value to companies in need of security programs and a fresh approach to understanding the treats facing modern complex systems.

Students interested in graduate work should refer to the Graduate and Professional Bulletin (http://catalog.colostate.edu/general-catalog/graduate-bulletin/).

Learning Objectives

Upon successful completion, students will be able to:

1. Dissect threats facing networked distributed systems, and multiple interacting networks, using current security practices.
2. Evaluate security engineering policies, principals, and controls to achieve a desired security posture for a complex organization.
3. Understand the security literature and how it applies to their research goals and the goals of their organization.
4. Create models of complex systems and the security controls used to protect them.