

Cybersecurity for Critical Infrastructure Certificate

Cybersecurity for Critical Infrastructure Certificate Requirements

23-24 credits

Code	Title	Hours
Required Courses		
IT 1100	Introduction to Unix/Linux	3
IT 2400 or MTRN 3600 & MTRN 3605	Intro to Networking (Prerequisite: IT 1100 and IT 1500, can be taken concurrently or MTRN 3500) Industrial Networks and Industrial Networks Lab	3
IT 2700	Information Security (Prerequisite: CS 1400, IT 1100, IT 1500, IT 2400 or CS 3150)	3
IT 3750	Industrial Control Systems Security (Prerequisite: IT 2700 and MTRN 2300)	3
MECH 1200 & MECH 1205 or CS 1400 & ECE 1200	Coding and Coding Lab (Prerequisite: MECH 1000) Fundamentals of Programming and Intro to Microcontrollers	4
MTRN 2300 & MTRN 2305	Introduction to Programmable Logic Controllers and Introduction to Programmable Logic Controllers Lab (Prerequisite: MECH 1200)	4
Total Hours		20

Code	Title	Hours
Elective Courses (Choose one course)		
SE 3250	Internet of Things Programming (Prerequisite: CS 1410)	3
IT 4510	Ethical Hacking & Network Defense (Prerequisite: CS 1400 and IT 3100)	3
MTRN 2350 & MTRN 2355	Advanced PLC Programming and Applications and Advanced PLC Programming and Applications Lab (Prerequisite: MTRN 2300)	4

Completion Requirements

1. Cumulative GPA of 2.0 or higher
2. Grade C or higher in all required courses.

Cybersecurity for Critical Infrastructure Certificate Program Learning Outcomes

At the successful conclusion of this program, students will be able to:

1. Evaluate cybersecurity risks associated with ICS and SCADA systems.
2. Apply appropriate mitigation strategies to industrial systems to enhance system security and resilience.
3. Influence technology selection and deployment based on security criteria.