SMART GRID CYBERSECURITY GRADUATE ACADEMIC CERTIFICATE

This academic certificate is offered by the Department of Electrical and Computer Engineering and is supported by the Computer Science Department's cybersecurity graduate program curriculum. Students will develop an understanding of power systems modeling, communication, control and its associated cybersecurity challenges. The offered courses cover theory and practice that help engineers identify and analyze threats and vulnerabilities to digital systems and networks and apply appropriate processes, tools, and mitigation strategies for improving cybersecurity.

All required coursework must be completed with a grade of B or better (O-10-b)

Code	Title	Hours
ECE 421	Introduction to Power Systems	3
ECE 544	Supervisory Control and Critical Infrastructure Systems	3
CYB 536	Advanced Information Assurance Concepts	3
Select 2 from the following:		**6**
ECE 422	Power Systems Analysis	
ECE 469	Resilient Control of Critical Infrastructure	
CS 587	Adversarial Machine Learning	
CS 543	Embedded Systems	
ECE 586	Industrial Control Systems	
Total Hours		**15**

Courses to total 15 credits for this certificate

1. Develop a solid understanding of the cyber vulnerabilities and risks to power systems.

2. Students should have the knowledge, skills, and abilities to be able to: (a) Understand organizational and/or cyber-system requirements, architecture, design, and implementation; (b) Describe and analyze the system with appropriate detail; (c) Develop a threat model; (d) Identify potential vulnerabilities; (e) Identify appropriate risk analysis processes and standards; (f) Perform risk analysis and assessment; (g) Identify, evaluate, design, apply, and document security and resiliency enhancements and risk removal or mitigation approaches, tasks, and security controls.

3. Learn how telecommunication systems and new sensors could be used to improve the power system cybersecurity.

4. Learn how to model power systems.