Georgia Institute of Technology
School of Electrical and Computer Engineering

ECE-8853 Cyber-Physical Security in Electric Energy Systems Fall 2020

Course Information

This course covers the cyber-physical infrastructure of electric energy systems and the technology and security practices to protect the operation of electric energy systems. It is intended to provide students with the ability to study the complex cyber-physical infrastructure for protection and control of electric energy systems, become familiar with communication protocols and standardization, identify cyber vulnerabilities of electric energy systems and learn how to protect against cyber-attacks and understand present practices for cyber security.

Time and Place: Expected: MWF 12:20-13:10, VanLeer C341

Instructor: A. P. Sakis Meliopoulos

Office: E-164, Phone: 404 894-2926
e-mail: sakis.m@gatech.edu
e-mail: sakis@comcast.net
Canvas and Course web site: http://home.comcast.net/~energia/

Office hours: MW 1:30 - 3:00 pm

Text: Class Notes
Conference and Journal Articles
A. P. Sakis Meliopoulos, *Power System Relaying: An Introduction* (980 pages)

Grading policy:

Homework	15 %
MidTerm Exam	15 %
Projects	3 each 15 %
Final	25 %

Projects: Details will be given at the following schedule: Sept 4, Oct 2, Nov 6.

General Info.: The midterm exam is closed book and closed notes. The final exam is take-home. Two formula sheets (8.5" x 11" paper, both sides) are allowed for the midterm exam. The formula sheet(s) should be handwritten originals. The final exam will be comprehensive, covering all topics presented.

Questions concerning grading of any assignment or exam must be presented to the instructor within one week after the grade is received. *No consideration will be provided after one week.*

Attendance: Class attendance is **strongly recommended**. It is understandable that occasionally a student may miss a class due to illness or a personal emergency. Students should consult the Georgia Tech policy on attendance at http://www.catalog.gatech.edu/rules/4/. It is the student's responsibility at all times to keep abreast of course announcements, consult the course web site, obtain handouts, etc. All homework, solutions, handouts, etc., will be posted on CANVAS and the course web site.

All absences from exams should be handled through the Office of the Vice President for Student Life and Dean of Students. Students must read the section “Attendance” of the above referenced link.

Course Objective: This course covers the cyber-physical infrastructure of electric energy systems and the technology and security practices to protect the operation of electric energy systems. It is intended to provide students with the ability to study the complex cyber-physical infrastructure for protection and control of electric energy systems, become familiar with communication protocols and standardization, identify cyber vulnerabilities of electric energy systems and learn how to protect against cyber-attacks and understand present practices for cyber security.

Prerequisites: Students should be familiar with time-domain and frequency domain circuit analysis, digital arithmetic, programming (any language), and with basics of embedded systems.

Homework: Homework will be collected on the due date provided on the first page of the homework. It is strongly recommended that you solve the homework individually; discussion in groups is also allowed provided that each student creates his/her own report. Copying or identical reports are not permitted. Late homework will be penalized. No homework will be accepted after solution is posted.

Academic Honesty: Georgia Tech aims to cultivate ethical behavior and avoid any form of academic misconduct, as defined in the Georgia Tech Academic Honor Code, which can be found in http://www.catalog.gatech.edu/policies/honor-code/ or http://www.catalog.gatech.edu/rules/18/. The policies will be enforced.

Accommodations: Students with learning needs that require special accommodations should contact the Office of Disability Services at (404)-894-2563 or http://disabilityservices.gatech.edu/, to discuss your special needs and to obtain an accommodation letter. Inform the instructor promptly and all help possible will be provided.

ECE8853	**Cyber-Physical Security in Electric Energy Systems**	**Fall 2020**

Introduction to Electric Energy Systems

- Overview
- Protection and Control Functions
- Generation, Transmission, Distribution, End Users
- Technology and SCADA Evolution
- Communication layers and standards
- Automation and cyber security standards

Cyber Security Vulnerabilities of Energy Systems

- Cyber threats to Electric Energy Systems
- Classification of attacks
- Cyber vulnerability of protection systems, operations, generation, others
- Threat level assessment
- Example attacks and effects (**project 1**)
- **Guest Speaker**: TBD

Substation Automation

- Protection and Control Functions
- Generation substation process control systems
- Optimization and Operation
- Authentication methods / standards
- Automation and Protocol Standards
- IEC61850 family of standards / cyber security
- Multi-Physics and Cyber co-modeling and simulation
- Attack detection methods
- Critical infrastructure protection (NERC)
- Virtual Testing (**project 2**)
- Substation Cyber Security standards and practices

Communications

- The seven layer OSI model
- Secure communications – Encryption
- Merging Unit to data concentrators
- Inter-IED communications
- Substation-substation, Substation-Control Center communications
- Inter-control center communications
- Distribution/End User communications
- System to Enterprise communications
- Protocols and Standards
- Access and authentication
- Security Practices
- Intrusion Detection Systems (**project 3**)
- **Guest Speaker**: TBD

Microgrids and Customer Energy Systems

Advanced Cyber-Physical Security Methods

- Malicious data attack detection and identification
- Malicious configuration files/settings attack detection
- Malicious control detection
- Industry standards and trends