A New Course, "Critical Infrastructure Security: The Emerging Smart Grid"

Anurag Srivastava, Carl Hauser, David Bakken, and M.S. Kim, Washington State University

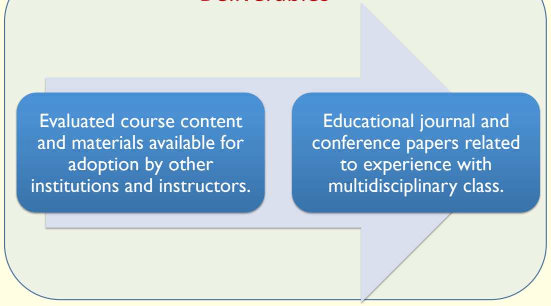
Overall objectives --

- Design a course with multi-disciplinary content including data communication, computing, control, cyber-security and power grid.
- Design a course to target audience of senior undergraduate and graduate engineering/ computer science students.
- Additionally, offer to online distance engineering students or engineers from industry.
- Design course materials to be easily adopted by instructors at other schools.
- Evaluate course outcomes and improve the content.

Workforce need for this education --

- With ongoing smart grid activities, there is a strong need for a workforce with interdisciplinary expertise to have sustained development and progress, specifically cyber-physical security.
- Curriculum at most universities have not yet been revised with ongoing smart grid initiative.
- The expectation is that the students completing this course are prepared to handle problems in smart grid cyber security based on their interdisciplinary expertise.

Deliverables --

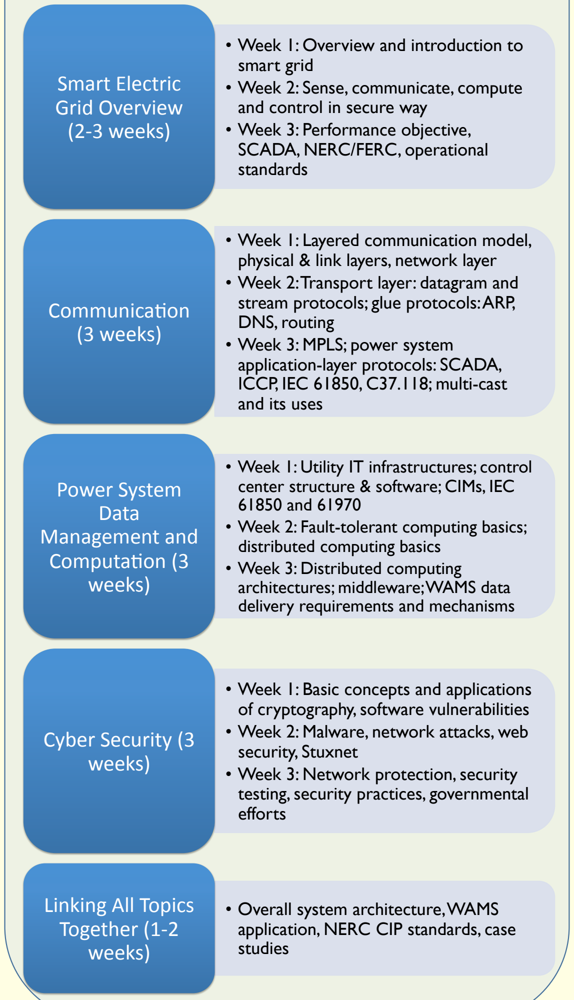


Evaluated course content and materials available for adoption by other institutions and instructors.

Educational journal and conference papers related to experience with multidisciplinary class.

Course Description --

Course Contents



Smart Electric Grid Overview (2-3 weeks)

- Week 1: Overview and introduction to smart grid
- Week 2: Sense, communicate, compute and control in secure way
- Week 3: Performance objective, SCADA, NERC/FERC, operational standards

Communication (3 weeks)

- Week 1: Layered communication model, physical & link layers, network layer
- Week 2: Transport layer: datagram and stream protocols; glue protocols: ARP, DNS, routing
- Week 3: MPLS; power system application-layer protocols: SCADA, ICCP, IEC 61850, C37.118; multi-cast and its uses

Power System Data Management and Computation (3 weeks)

- Week 1: Utility IT infrastructures; control center structure & software; CIMs, IEC 61850 and 61970
- Week 2: Fault-tolerant computing basics; distributed computing basics
- Week 3: Distributed computing architectures; middleware; WAMS data delivery requirements and mechanisms

Cyber Security (3 weeks)

- Week 1: Basic concepts and applications of cryptography, software vulnerabilities
- Week 2: Malware, network attacks, web security, Stuxnet
- Week 3: Network protection, security testing, security practices, governmental efforts

Linking All Topics Together (1-2 weeks)

- Overall system architecture, WAMS application, NERC CIP standards, case studies

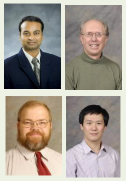
Learning Objectives

- Trained students, ready to contribute to security aspects of industrial projects related to the electric grid.
- Students will be able to understand vulnerabilities and the threats to the power grid and associated infrastructure

Delivery Methods

- In class Tegrity ANGEL LEARNING
- Online using Angel and Tegrity tools available at WSU

Teaching Faculty Members



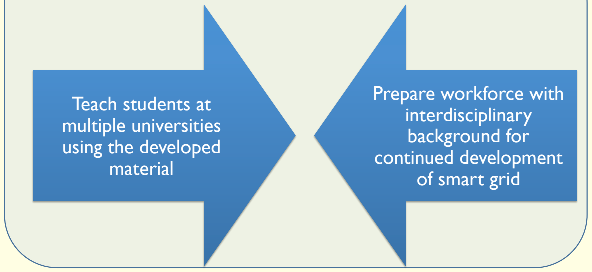
Team taught by 4 faculty members:

i) Anurag Srivastava (Power Grid),
ii) Carl Hauser (Communication)
iii) Dave Bakken (Data Management/ Computation)
iv) Min Sik Kim (Cyber Security)

Course Evaluation

- Students feedback and evaluation of course
- Student performance based on 8 assignments, 2 quiz, 1 mid term take home exam, 1 final take home exam, and 1 final project

Potential uses of this course --



Teach students at multiple universities using the developed material

Prepare workforce with interdisciplinary background for continued development of smart grid