Dr. F. Karaa Fall, 2016

CE 672-101: Critical Infrastructure II

Security Management of Infrastructure Systems

Class Hours

Tuesday 6:00 PM - 9:05 PM in CKB 315 (first day of class is September 6, 2016)

Office Hours (Colton 274)

Tue 5:00 PM- 6:00 PM and Wed 4:00 PM-5:30 PM or by e-mail or appointment
at (973) 642-4198 or karaa@njit.edu

REQUIRED TEXT

The required text for this course is Ted Lewis's Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 2nd Edition. (ISBN: 978-1-118-81763-6
400 pages, November 2014, ©2015, Hoboken, N.J.: Wiley & Sons.)

Other files are assigned electronically as supplemental readings and will be e-mailed to class participants. These are denoted in course outline as Efiles.

COURSE DESCRIPTION:

This course focuses on the areas of vulnerability assessment and security management of critical infrastructure systems through the development of risk and resilience models applied to various critical infrastructure networks. The first section of the course is policy related and starts out with a review of the critical infrastructure sector history and hierarchy, and strategies and challenges facing the critical infrastructure now developing field. It also goes over the evolution of the National Infrastructure Protection Plan (NIPP) from a pure protection focus, to one that goes beyond protection to resilience (through effective response and mitigation). The overarching goal is to build an analytical framework for vulnerability and security management of infrastructure systems in its key aspects: prevention, warning/detection and event mitigation and response planning and execution.

The course starts with a historical review of policy and origins of the field of critical infrastructure protection. Next, the modeling of topography, hazards, risk and resilience under a range of assumptions and mathematical/probabilistic theories is covered. The goal is to familiarize students with an adaptable analytical framework to uncertainty and risk analysis, which includes applied techniques for facility and network modeling and performance simulation under various hazards and sector-specific approaches to vulnerability and risk analysis. In particular, the study and application of a Model-Based Risk Analysis (MBRA) approach initially developed in the early 2000's as the MBVA (Model-Based Vulnerability Analysis) for application to critical infrastructure protection will be presented as an example of network-based analysis. Additionally, other analytical and probabilistic techniques are reviewed to get a detailed representation of local and network risk and elements of the resilience equation to be factored in a resilience improvement program.

In the second part of the course, following the review of analytical network risk and resilience techniques, a sector-based approach is taken for the review of physical critical infrastructure systems including water supply/environmental, transportation, power and fuel systems, SCADA (Supervisory Control and Data Acquisition and Telecommunications) systems, and telecommunications. We will analyze basic elements of these systems; identify their vulnerability to breakdown due to accidents, natural disasters, or terrorist attacks; and examine best practices used to reduce these vulnerabilities, databases and information systems available for some of these infrastructure systems. We will focus on developing systems analyses and models of the infrastructures and on strategic responses to breakdown scenarios, including the use of MBVA.

In both the first part dedicated to modeling, and the second one, which is sector-specific, the course will introduce a range of related topics including condition assessment and monitoring, network performance measures, integrated risk measures combining economic cost to public health, long-term v/s short-term risk mitigation, operational and analytical capabilities, pre-event risk mitigation techniques and real-time response to natural and man-made hazards.

LEARNING OUTCOMES

When you have completed this course, you will be able to

- have a basic understanding of how infrastructure systems work, and the impact of policy on their evolution;
- understand the various types of risk and probability theories applied to infrastructure system hazards, performance risks and extreme events;
- identify and explain the major challenges to critical infrastructure protection;
- explain network theory and compare and contrast with classical systems theory;
- define and apply basic network theory concepts, such as trees, nodes, cascade Networks and differentiate between scale-free and small world network topologies;
- identify and describe the steps in some of the major analytical approaches, such as the MBRA and MBVA (Model Based Risk Analysis and Vulnerability Analysis);
- apply probabilistic risk and resilience models to an infrastructure system, adapted to the appropriate network topography and type of hazards;
- analyze the applicability and limitations of an approach such as MBVA to the analysis of risk, resilience of an infrastructure system;
- explain how the economic and lifecycle characteristics of an infrastructure system affect its vulnerability;
- identify major components, hubs, and links, vulnerabilities, major threat scenarios, and best practices for each of the infrastructure systems covered in this course;
- for each of the infrastructure systems, identify and describe interdependencies with other systems, and organizational and human resources challenges;
- identify and evaluate methods for obtaining estimates of the probability of different threats, and apply multi-criteria analysis to the problem of security and protection management of critical infrastructure.

COURSE OUTLINE (Subject to updating throughout semester)

Week	Date	Textbook/Reading	Assignment	Topics
1	6 Sep	Lewis, Chapter 1: Origins, National Infrastructure Protection Plan (Moodle), Presentation on Origins	Moodle: Questions on NIPP and "Potholes and Detours"	Origins of Critical Infrastructure Protection

2	13 Sep	Lewis, chapter 1 (ctd.), Origins, Challenges, Organization, Efiles		Critical Infrastructure Origins and Challenges
3	20 Sep	Efiles	Problem or CI Organization Strategy	Federalism, Situational Awareness
4	27 Sep	Chapter 2, Overview of Risk Models and Networks, Efiles	Moodle Assignment on Network Models	Network Theory and Model Applicability to Critical Infrastructure
5	4 Oct	Chapter 2 (ctd.), MBRA, Efiles	Moodle Assignment on fault Trees, risk minimization	Fault-Tree Model and risk evaluation
6	11 Oct	Appendix A, Handout of Bayesian Modeling	Bayesian Updating	Bayesian Statistics, Bayesian Reasoning
7	18 Oct	Chapter 4 (Network Topology, Complex CIKR Systems), Efiles,	Moodle Assignment on Risk Modeling (Part1)	Risk Analysis; Network Availability Strategies
8	25 Oct	Appendix B: Advanced Mathematical Modeling (Risk And Resilience)	Moodle Assignment on Risk Modeling (Part2)	Risk and Resilience; Application of Risk Analysis and Resource Allocation Model Selected
9	1 Nov	Chapter 3 (Theories of Catastrophe), and Mid-term review	Sector Project Definition (part 1)	
10	8 Nov			Mid-Term
11	15 Nov	Chapters 5, 6, and 7 (Communications, Internet, CyberSecurity), Chapter 15 Transportation		Definitional Stage (part 1)
	22 Nov	No meeting	Thursday Schedule	Thanksgiving Week
12	29 Nov	Chapters 10, 11, 12 and 13 (SCADA, Water/WW, Energy, Power)		Definitional Stage (part 1)
13	6 Dec	Chapters 5, 6, and 7 (Communications, Internet, CyberSecurity), Chapter 15 Transportation		Integrated Presentations (Part 2)
14	13 Dec	Chapters 10, 11, 12 and 13 (SCADA, Water/WW, Energy, Power)		Integrated Presentations (Part 2)

GRADING:

In addition to a mid-term and assignments from the textbook, the class will be divided in sector "projects" led by a student focusing applying course content and latest individual research to the assigned sector. Part of each sector, assignment is to be integrator of the state of the art in sector resilience in a formal presentation on their researched sector, and to write a synthesis paper on sector vulnerability analysis and reduction strategies.

The overall term grade will be based on the following elements:

Paper/Presentation: 40% (50% written paper/50% communication and presentation)
Homework and Class Participation: 30%
Mid-Term: 30%