

Course Number: XXXXXX

Course: Critical Infrastructure Protection Systems Analysis

University of XXXXXX

Fall/Spring Semester 20XXXXXX

NAME OF SCHOOL:

DEPARTMENT:

PROFESSOR:

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

COURSE DESCRIPTION/OVERVIEW:

In a single word, the term “infrastructure” represents all the basic physical and organizational structures needed for the operation of a society or enterprise. Infrastructure is built by humans to satisfy human needs. Infrastructure is social — its operation and use is driven by social customs, needs, and traditions. Infrastructure is also technological — it relies on numerous technologies, some simple, others advanced — to perform its function well or even at all. Infrastructure and society are intertwined — society drives infrastructure, and infrastructure shapes society.

In order for us to fully appreciate the relationship between infrastructure and the society that depends on it, we must be able to think of this connection as a system of systems. In its most general sense, a system is a collection of things that interact with one another to serve some particular purpose or perform some function. We must appreciate infrastructure as part of the larger system of satisfying human needs. We must look at infrastructure as a collaboration between technologies and humans to deliver essential services that society depends on. The general notion of “critical infrastructure” can be divided into multiple sectors, each of which interacts and collaborates with the other in multiple, and potentially unpredictable ways. These sectors can be further divided into segments, assets, parts, and so on. We must understand the nature of interaction between parts of a system at all levels in order to fully appreciate the role each individual part and subsystem plays in making our infrastructure work; this knowledge is prerequisite to understanding how the compromise of one or more of these parts impacts the entire system, for better or for worse. And, we must anticipate how both society and infrastructure will evolve together to meet future challenges.

This course focuses on systems analysis in the context of critical infrastructure

protection. This is a theoretical course, but the tools taught will be applied in practical ways. Building on the learner's prior knowledge of the different segments of critical infrastructure, this course will introduce the notion of a system and apply it to better understand how infrastructure works and how it can fail and not fail under stress. This course will provide the student with tools and techniques for describing systems in terms of its internal parts and dependencies with other systems, studying systems, and uncovering risks affecting systems. A number of analytical techniques will be discussed, including divergent/convergent thinking, hierarchical holographic modeling (HHM), functional block diagrams, fault tree analysis, and event sequence diagrams. While this course is largely technical in nature, it is geared toward learners from non-engineering backgrounds. Mathematical concepts will be presented to the extent needed to apply the techniques introduced in class.

CREDITS CONFERRED: 3

PREREQUISITE: Introduction to Critical Infrastructure Protection and Resilience

LEARNER OUTCOMES/OBJECTIVES (AS MAPPED AGAINST DEPARTMENT OF HOMELAND SECURITY CRITICAL INFRASTRUCTURE CORE COMPETENCIES):

This course is designed to enable learners to:

1. **Define** the following terms in the context of critical infrastructure protection: system, interdependency, failure, cascading failure, common cause failures, success, inputs, outputs, state variables, feedback, and others as introduced.
2. **Explain** the fundamentals of the following concepts: the Eight Elements of Thought, nine Intellectual Standards, basic logic, and basic probability theory.
3. **Discuss** how systems analysis fits within a risk management framework.
4. **Decompose** a system into its basic elements, describing what it does, why it is needed, how it works, and all relevant interdependencies.
5. **Apply** the following structured analytic techniques to understand and assess the performance of real systems: divergent/convergent thinking, hierarchical holographic modeling, reliability block diagrams, failure modes and effects analysis, fault tree analysis, event tree analysis, and pros/cons, among others.
6. **Discuss** the current state of systems research for critical infrastructure protection, including key contributors, periodicals, and research institutions.
7. **Identify and appraise** vulnerabilities in simple infrastructure systems.
8. **Identify** opportunities for advanced study in systems analysis.

DELIVERY METHOD/COURSE REQUIREMENTS:

This is a graduate level course in systems analysis for non-engineers. Yet, this course is a technical course that will require the learner to master technical topics. This course focuses on applying theory to practical applications. The course will consist of readings as directed, class participation, take-home assignments, and two research projects. In-class activities will consist of case studies, simulation, and other group activities.

The assigned course readings include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office, Congressional Research Service, etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

GENERAL COURSE REQUIREMENTS:

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Since class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. According to university policy, all beepers and cell phones should be turned off before class begins.

GRADING:

The following provides an approximate breakdown of how each assignment contributes to the overall performance in the class.

Class Attendance and Participation	25%
Weekly Take-home Assignments (nine)	25%
Systems Analysis Mid-Term Project	25%
Risk Analysis Final Project	25%

ACTIVITIES, EXERCISES, AND RESEARCH PROJECTS:

1. Systems Analysis Mid-Term Project (25%):

Prior approval of the topic for the systems analysis midterm project is required.

Learners should submit a one-paragraph written description of their proposed topic in class or via email for approval no later than the beginning of Lesson 3.

All learners will apply their knowledge of systems analysis to describe, in a manner that is comprehensible to a layperson, how a real system works. To this end, learners will present to the instructor a detailed description of a real infrastructure system. Each learner will work individually with the instructor to select a system for this project. Learners will start by defining the boundary conditions of the system, identifying all relevant stakeholders and their concerns, system objectives, constraints, inputs, outputs, and state variables. Then, learners will identify the primary and secondary components of the system and how they interact to make the system work. In addition, learners will describe how their system interacts with other systems, to include the extent to which it is dependent on or essential for other systems to work properly. All data used for this assignment will be properly cited; when data is unavailable, all assumptions with justification will be articulated.

There are two deliverables for this project. The first is a comprehensive written report describing precisely what the system is, what it does, how it works, and how it is monitored. This report may be as few as five pages, or as long as 30 pages. The key is that the description of the system must be complete within its defined scope. It is up to the learner to package the report so that it is comprehensible; however, it should consist of the following elements: system definition, summary of stakeholders and their perspectives on the system, block diagram of the system and description of all parts, pertinent historical incidents affecting similar systems, relationships with other systems, inputs, outputs, state variables, and strategies for monitoring performance. In addition, the learner must carefully document all data and information used, as well as any assumptions made to compensate for missing data. The second deliverable is a short YouTube style video that presents to a layperson a comprehensive, yet accessible summary of the system chosen by the student. This video shall be no less than five minutes and no more than eight minutes in duration. The video may be highly edited and created using sophisticated equipment (e.g., high-definition camcorder with carefully prepared script and edited with Final Cut Pro), or it may simply be a narrated slide-based presentation (e.g., power point presentation narrated using Camtasia). Both deliverables are due to the instructor prior to the start of **Lesson 8**.

Note: Individual instructors will establish clear criteria for passing and failing this mid-term project assignment. If a student does not satisfy criteria for pass, but also does not satisfy criteria for fail, the student will have two weeks to fix the assignment. Recommended criteria for passing or failing the mid-term project assignment are provided as follows.

PASS Criteria		FAIL Criteria	
	Uses complete sentences throughout		Incomplete submission (missing parts, and blank responses)
	System description complete within defined scope		Does not follow submission instructions
	Adequately defines the system		Did not obtain prior approval from instructor during Lesson 3
	Identifies and describes all relevant stakeholders and perspectives		Does not provide YouTube video to accompany written report
	Provides a fully-described block diagram of the system		Late submission
	Provides an account of historical incidents afflicting similar systems		
	Provides coherent and reasoned responses to all questions.		BLANK
Final Assessment			
PASS	FIX Resubmit by:	FAIL	

2. Risk Analysis Final Project (25%):

This project provides learners an opportunity to leverage their expertise to conduct a comprehensive risk assessment of a particular system. For this project, learners will leverage the systems they studied for their mid-term project, incorporating instructor comments where appropriate. Learners will use their knowledge of their chosen system to systematically identify vulnerabilities, describe the types of threats that could exploit these vulnerabilities, and estimate how compromising the system will adversely affect the interests of one or more stakeholders. Moreover, learners will identify at least two alternative options for mitigating system vulnerabilities (in addition to the “do nothing” option) and evaluate them in terms of their costs and ability to reduce risk.

As with the midterm project, there are two deliverables associated with this project. The first is a comprehensive written risk analysis report that summarizes in full detail the results from this study. This report shall include as its first part a comprehensive description of the system developed for the midterm project that incorporates any recommended changes or fixes made by the instructor. The second part will present a summary account of all identified vulnerabilities within the system scope, postulated threats that could exploit these vulnerabilities, and estimated impacts to stakeholder interests should the system be exploited. The third part will evaluate the pros and cons of alternative mitigation strategies in terms of their ability to reduce risk through vulnerability reduction.

The second deliverable consists of a 5-minute in-person presentation aimed at convincing stakeholders to pursue one of the risk mitigation options considered. Hence, this deliverable must describe the alternatives and justify their benefits using sound argumentation informed by the results of risk analysis. The final project will be presented to the class of “stakeholders” during the last class meeting (Lesson 15).

Note: Individual instructors will establish clear criteria for passing and failing this final project assignment. If a learner does not satisfy criteria for pass, but also does not satisfy criteria for fail, the learner may be given two weeks to fix the assignment at the instructor's discretion. Learners are encouraged to engage with the instructor one or more times prior to final submission for feedback and critique. Recommended criteria for passing or failing the final project assignment are the same as for the mid-term project.

3. Take Home Assignments (25%):

Each week, the instructor will assign small-scale problems aimed at helping learners better understand class concepts. The time burden for each problem set is expected to not exceed four hours. Example problems include developing a simple functional block diagram or fault tree for a system, critically evaluating assigned readings, developing a pro and con list for different countermeasures, etc. There will be nine take-home assignments spread across the semester.

4. Expectations for Participation (25%):

Participation includes coming to class prepared, participating in class discussion, participating in class exercises, and reflecting on the experience after class by way of a private journal to be submitted at the end of the semester. To achieve full credit for participation, learners must attend, participate, and reflect. Learners are expected to attend all classes; however, learners are permitted to miss two class sessions without it adversely affecting his/her final course grade.

INCORPORATION OF FEEDBACK:

The course instructor will provide multiple opportunities for learners to provide constructive feedback on course delivery and content over the period of the course. These may be in the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to provide written feedback following each assignment, to include general feedback on the course or specific feedback on an individual assignment. On-line feedback is also encouraged throughout the course, either through email or a course web forum. Finally, the instructor will provide written feedback to the learners on all assignments.

COURSE TEXTBOOKS:

There is no single textbook available that can address the instructional needs for this class. Consequently, the course will assign readings collected from multiple print and online resources and make these available for download or for purchase as a collection of articles and book chapters.

GRADING SCHEME: SCHOOL POLICY DEPENDENT

COURSE OUTLINE

The following outlines the 15-week course agenda. Each lesson, starting with Lesson 2, focuses on the theoretical basis for practical analytical tools (shown in parenthesis).

Lesson / Week	Topic	Deliverables
1	Course overview, review of critical infrastructure protection sectors, and the fundamentals of risk management (the nine questions of risk management)	None
2	Critical thinking and foundations of analysis (Eight Elements of Thought, Intellectual Standards)	Assignment 1
3	The multiple views of a system and basic terminology (hierarchical holographic modeling, scoping a systems analysis)	Assignment 2
4	Elements of a system, block diagrams, and describing systems and interdependencies (reliability block diagrams)	Assignment 3
5	Identifying system weaknesses (failure modes and effects analysis, anticipatory failure determination)	Assignment 4
6	Logic and systems (fault trees and success trees)	Assignment 5
7	System performance (event trees)	Assignment 6
8	Review and discussion of videos and special topics as appropriate	Mid-term Project
9	Quantifying system performance (descriptive statistics)	Assignment 7
10	Threats to systems (divergent/convergent thinking)	Assignment 8
11	Impacts of system incidents (multi-attribute utility theory, pair-wise ranking)	None
12	Protecting systems and benefit-cost analysis (pros/cons/fixes)	Assignment 9
13	Monitoring system performance (indications and warnings analysis)	None
14	System evolution and course wrap-up (technology futures analysis)	None
15	Final project presentations	Final Project (due Sat @ 11p)

LESSON 1 TOPIC: COURSE OVERVIEW AND REVIEW OF CRITICAL INFRASTRUCTURE PROTECTION AND RISK MANAGEMENT

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Describe the scope of the course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes
- Articulate the nine fundamental questions of risk management spanning risk assessment, risk communication, and risk control
- Discuss various infrastructure sectors and their importance to different people
- Distinguish between what constitutes a threat, vulnerability, and consequence from different perspectives

2. Rationale:

This first lecture aims to introduce and review essential concepts of risk and establish the motivation for learning about systems analysis. This lecture also introduces the critical topic of perspective and illustrates how perspective affects points of view about systems and risk.

3. Discussion Questions:

- Is there a difference between systems analysis and risk analysis?
- What types of analysis is required to answer each of the nine questions of risk?
- How does the quality of your understanding about a system affect the quality and credibility of your analysis?
- What role do perspectives play in labeling a particular event or phenomenon as a threat, vulnerability, or consequence?
- How does the U.S. Department of Homeland Security (DHS) break down infrastructure into different sectors and segments?
- What makes a particular infrastructure “critical”?

4. Class Agenda:

Activity	Duration
Review the syllabus	45 minutes
Discuss the nine questions of risk	45 minutes
In-class HVC activity	45 minutes
Review of infrastructure sectors	45 minutes
Total	180 minutes

5. In-Class Activity: The HVC Activity:

In this activity, the instructor will present to the learners a set of 8-10 images depicting some sort of situation. For each, the student will be asked to identify whether what they are seeing is a hazard, vulnerability, or consequence (HVC), and from whose perspective is it seen that way. The goal of this activity is to illustrate that any particular situation can be seen as a hazard, vulnerability, or consequence depending on the particular point of view.

6. Required Reading:

J. O. Matschulat, "An Introduction to the Concept and Management of Risk," in Johnson, T. A. ed. *National Security Issues in Science, Law and Technology*, CRC Press, 2005, 291-357.

R. R. Lochry, R. D. Hensley, P. Flammer, D. R. Smith, R. G. Head, E. M. Henry, W. R., Nelson Hodson III, E. B., G. G. Carson, and J. F. Guilmartin, "Final Report of the USAF Academy Risk Analysis Study Team," 1971, AD-729-223.

U.S. Department of Homeland Security, "DHS Infrastructure Taxonomy," Version 3. 2008. Available at: <http://www.hsdl.org/?view&doc=133262&coll=limited>.

U.S. Department of Homeland Security, "Risk Lexicon," 2010. Available at: <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

The instructor may include additional readings on the philosophy of risk management for infrastructure protection. Such papers include:

Y. Y. Haimes, "Total Risk Management," *Risk Analysis*, 11, 1991, 169-171.

G. Manunta, *Security and Methodology*, Diogenes Papers No. 2, 1999, See: <http://www.srsi.org/diogenes.htm>.

7. Additional Recommended Reading:

President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," 1997. Available at: <http://www.fas.org/sgp/library/pccip.pdf>.

U.S. Department of Homeland Security, "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency," 2009. Available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

White House, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," 2003. Available at: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

G. W. Bush, "Critical Infrastructure Identification, Prioritization and Protection," HSPD-7, 2003. Available at: <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>.

8. Deliverables for Today:

None

9. Assignment for Next Time:

Take-home Assignment #1: Produce a 500-1000 word paper describing a particular

critical infrastructure asset. Describe the asset in terms of what it does, what infrastructure(s) it supports, who the stakeholders are, and their interests in the asset. For one of these stakeholders, provide three examples of what constitutes a threat, vulnerability, and a consequence.

LESSON 2 TOPIC: CRITICAL THINKING FOR SYSTEMS ANALYSIS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Recite and explain the Eight Elements of Thought, the Intellectual Standards, and DHS analytic tradecraft standards
- Apply the Eight Elements of Thought and Intellectual Standards as tools to deconstruct and appraise the quality of a selected published infrastructure risk assessment or analysis article

2. Rationale:

This lecture will introduce the topic of critical thinking to system analysis learners. Being able to think critically is essential for performing high-quality analysis work in any field, including the study of systems.

3. Discussion Questions:

- What role does the Eight Elements of Thought and Intellectual Standards play in systems analysis?
- How can concepts from critical thinking be applied to enhance the quality of analysis?
- How can concepts from critical thinking be applied to appraise others' analyses?

4. Class Agenda:

Activity	Duration
Presentations and discussions of Assignment #1	25 minutes
Discuss the DHS analytic tradecraft standards	45 minutes
Discuss the Eight Elements of Thought and Intellectual Standards	20 minutes
In-class assessment appraisal activity	45 minutes
Discussion of the activity	45 minutes
Total	180 minutes

5. In-Class Activity: Assessment Appraisal Activity:

In this activity, the instructor will provide learners with a short, but comprehensive risk assessment of foreign infrastructure or resources. Learners will be asked to read the assessment, deconstruct the analysis using the Eight Elements of Thought as a guide, and appraise the analysis using the Intellectual Standards. Example risk assessments include a recently declassified Central Intelligence Agency (CIA) assessment entitled “Western Platinum Dependence: A Risk Assessment,” (1985). The entire activity will be completed in-class. The goal of this activity is to provide learners with practice reading, decomposing, and appraising the results of an analysis pertaining to critical infrastructure.

6. Required Reading:

R. Paul and L. Elder, *The Miniature Guide to Critical Thinking: Concepts and Tools*,

Foundation for Critical Thinking, 2009.

T. L. Norman, *Risk Analysis and Security Countermeasure Selection*, CRC Press, 2009, 67-81.

A. Langley, "Between 'Paralysis by Analysis' and 'Extinction by Instinct'," *Sloan Management Review*, 36 (3), 1995, 63-76.

7. Additional Recommended Reading:

Director of National Intelligence, Intelligence Community Directive 203 (ICD-203): Analytic Standards, 2007. Available at: <http://www.fas.org/irp/dni/icd/icd-203.pdf>.

8. Deliverables for Today:

Take-home Assignment #1

9. Assignment for Next Time:

Take-home Assignment #2: Find a recent article published in a reputable newspaper that focuses on some aspect of critical infrastructure protection. Use the Eight Elements of Thought to decompose the argument of the article. Use the Intellectual Standards to appraise the article. Come prepared to discuss your article in the next class.

LESSON 3 TOPIC: MULTIPLE PERSPECTIVES OF LARGE-SCALE SYSTEMS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: large scale system; objectives; values; dependency; and interdependency in addition to other pertinent terms
- Explain constructivism, realism, reductionism, and holism in the context of systems analysis
- Apply the hierarchical holographic modeling (HHM) methodology to understanding different competing perspectives on a single system
- Explain the concept of a security context and properly develop a system scope for further study

2. Rationale:

This lecture introduces the concept of a system being a human construct, and that what constitutes a system is highly dependent on point of view. This lecture starts with the philosophical ideas of constructivism vs. realism and then proceeds to apply practical tools to assist the learners in seeing particular objects from multiple viewpoints.

3. Discussion Questions:

- What is the difference between constructivism and realism? How does each affect the way in which we study systems?
- What is the difference between reductionism and holism? How does each affect the way in which we study systems?
- What role does “point of view” play in defining a system?
- How does defining a “security context” help in establishing a system scope?
- How can HHM be used to model multiple competing security contexts?
- How does system definition affect the interpretation of the term “interdependency”?

4. Class Agenda:

Activity	Duration
Presentations and discussions of Assignment #2	30 minutes
Lecture on theories of systems	45 minutes
Introduction to HHM and the Security Context	30 minutes
In-class HHM exercise	45 minutes
Presentation and discussion of group HHMs	30 minutes
Total	180 minutes

5. In-Class Activity: HHM and the Security Context:

In this activity, the instructor will provide learners with an image of an object, asset, etc. that is part of one or more systems. In groups of 2 or more (the particular group size is at the discretion of the instructor), learners will construct a three-level HHM characterizing as many security contexts as possible that relate to the image. Learners will then choose three specific security contexts and for each specify the corresponding scope of the

systems analysis that should be performed to support the associated decision makers (protectors). The goal of this assignment is to instill an appreciation for the constructivist viewpoint on systems, and to provide learners with practice looking at a particular asset from multiple perspectives.

6. Required Reading:

G. J. Klir, *Facets of Systems Science*. Springer, 2001, Excerpts from pages 3-87.

Y. Y. Haimes, *Risk Modeling, Assessment and Management*, 3rd Edition. Wiley, 2009, 90-153.

G. Manunta, *Defining Security*, Diogenes Papers No. 1, Cranfield Security Centre. 2000. Available at: <http://www.srsi.org/download/Diogenes%201.zip>.

L. A. Cox, *Risk Analysis: Foundations, Models and Methods*, Springer, 2001, 8-10.

7. Additional Recommended Reading:

R. Paul and L. Elder, *The Miniature Guide to Critical Thinking: Concepts and Tools*, Foundation for Critical Thinking, 2009.

S. Ramo and R. K. St. Clair, *The Systems Approach: Fresh Solutions to Complex Problems Through Combining Science and Practical Common Sense*, TRW, Inc., 1998. Available at: <http://www.incose.org/productspubs/doc/systemsapproach.pdf>.

8. Deliverables for Today:

Take-Home Assignment #2

Chosen system/topic for Systems Analysis Mid-Term Project

9. Assignment for Next Time:

Take-home assignment #3: Identify a critical infrastructure asset that you are somehow familiar with and construct a HHM describing the various security contexts that can be associated with the asset. For each security context, identify at least two relevant (though notional) vulnerabilities of interest to the protector in that context. For this assignment, you may revisit the critical infrastructure asset you studied for Take-home assignment #1.

LESSON 4 TOPIC: THE ELEMENTS OF A SYSTEM

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: elements; relations; inputs; outputs; states; objectives; constraints; exogenous variables; random variables; reliability; vulnerability; and success scenario
- Describe a system in terms of its objectives, constraints, input/output/state variables, elements, and relations among the elements
- Construct reliability block diagrams of simple systems and use them to identify potential vulnerabilities and single-point failures

2. Rationale:

This lecture builds on the previous lecture by providing learners with guidance on how to describe and diagram a system whose scope is fully specified. This is also the first lecture in which vulnerability/system failure is discussed.

3. Discussion Questions:

- Why is it important to describe a system in terms of its elements and relations?
- Why is it important to discuss how systems work in terms of objectives, constraints, and variables?
- What is the relationship between “objectives” and point of view?
- How can knowledge of the elements and relations be used to construct reliability block diagrams?
- What is the relationship between “exogenous variables” and infrastructure interdependencies?
- How can reliability block diagrams support vulnerability assessment?

4. Class Agenda:

Activity	Duration
Presentations and discussions of Assignment #3	30 minutes
Lecture/discussion on the properties of systems and relational analysis	45 minutes
In-class systems description exercise	75 minutes
Presentation and discussion of group systems	30 minutes
Total	180 minutes

5. In-Class Activity: Systems Description Exercise: In this exercise, the instructor will provide a short description of an infrastructure system from a particular point of view. Then, learners will describe the system in terms of its objectives, constraints, input variables, state variables, and output variables. Learners will also articulate the success scenario for the system. Learners will identify all relevant parts of the system and describe how they are related to one another using natural language. Then, learners will use these descriptions to construct the corresponding reliability block diagram. The goal of this exercise is to provide learners with hands-on experience describing real systems.

Learners will then use this description to create simplified models of how the system works.

6. Required Reading:

Y. Y. Haimes, *Risk Modeling, Assessment and Management*, 3rd Edition, Wiley, 2009, Excerpts from pages 57-88.

G. J. Klir, *Facets of Systems Science*, Springer, 2001, Excerpts from pp. 3-87.

A. Sonnenberg, J. M. Inadomi, and P. Bauerfiend, "Reliability Block Diagrams to Model Disease Management," 19 (2), 1999, 180-185.

S. Kaplan, Y. Y. Haimes, and B. J. Garrick, "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and the Resulting Refinement to the Quantitative Definition of Risk," *Risk Analysis*, 21 (5), 2001, 807-819.

7. Additional Recommended Reading:

U.S. Department of Homeland Security, "Risk Lexicon," 2010. Available at: <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

8. Deliverables for Today:

Take-Home Assignment #3

9. Assignment for Next Time:

Take-home Assignment #4: Identify a critical infrastructure asset that you are somehow familiar with and use it to define a system. You may build on the results from your previous assignment, or construct a completely new system. For this system, identify at least three of each of the following: objectives, constraints, inputs, outputs, and state variables. Then, identify all relevant elements of the system, describe how they interact with one another, and attempt to draw a block diagram of this system. Finally, identify at least two systems that are dependent on this system *and* two systems that this system is dependent on. Explain the nature of these dependencies.

LESSON 5 TOPIC: IDENTIFYING WEAKNESSES IN A SYSTEM

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: vulnerability and failure
- Explain the procedure for conducting a failure modes and effects analysis (FMEA)
- Explain the procedure for conducting an anticipatory failure determination analysis (AFDA)
- Apply FMEA and AFDA to identify the weaknesses of a selected infrastructure system
- Apply critical thinking skills to discuss pitfalls in the FMEA and AFDA approaches and explore ways to extend these analytic techniques

2. Rationale:

At this point in the class, learners should be starting to think clearly and critically about what a system is, how it can be described, and illustrated. This lecture expands on systems thinking by having learners apply their knowledge of systems to uncover weaknesses that can cause a system to fail or perform inadequately. To do this, this lecture introduces two new analytic techniques for learners to experience.

3. Discussion Questions:

- What kind of analysis is a prerequisite to performing a FMEA or an AFDA?
- How does FMEA/FMECA and AFDA compare to risk assessment in general?
- What are the pitfalls associated with performing a FMEA or AFDA?
- How does FMEA/FMECA or AFDA results fit within the scope of a systems analysis?
- In what ways can FMEA or AFDA be modified to support extended analysis of a system?
- Is FMEA or AFD the same as a vulnerability assessment? Why or why not?

4. Class Agenda:

Activity	Duration
Presentations and discussions of Assignment #4	30 minutes
Lecture/discussion on FMEA	15 minutes
FMEA exercise	45 minutes
FMEA debrief and discussion of the procedure	15 minutes
Lecture/discussion of AFDA	15 minutes
AFDA exercise	30 minutes
AFDA debrief and critical analysis of methods	30 minutes
Total	180 minutes

5. In-Class Activity: FMEA/AFDA Exercise:

In this exercise, the instructor will use the classroom as the basis for defining a system

(i.e., the “classroom system.”). From here, learners will fully specify the system and conduct a full FMEA of the system. Following the debriefing part of this exercise, learners will proceed to conduct an AFDA of the system. The goal of this exercise is to provide learners with an opportunity to practice using both FEMA and AFDA to uncover weaknesses in a system.

6. Required Reading:

American Society for Quality, “Failure Modes and Effects Analysis (FMEA),” 2011. Available at: <http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html>.

U.S. Department of Defense, “Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis,” MIL-STD-1629A, 1980. Available at: http://www.goes-r.gov/procurement/antenna_docs/reference/MIL-STD-1629A.pdf.

Resource Engineering Inc., “FMEA Pitfalls and Limitations,” 2011. Available at http://www.qualitytrainingportal.com/resources/fmea/fmea_pitfalls.htm.

S. Kaplan, S. Visnepolschi, B. Zlotin, and A. Zusman, “New Tools for Failure and Risk Analysis: An Introduction to Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring,” Ideation International, 1999.

Ideation International, “AFD (Anticipatory Failure Determination),” 2011. Available at: <http://www.ideationtriz.com/AFD.asp>.

J. B. Bowles, “An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis,” *Proceedings of the 2003 Annual Reliability and Maintainability Symposium*, 2003, 380-386.

7. Additional Recommended Reading:

R. E. McDermott, R. J. Mikulak, and M. R. Beauregard, *The Basics of FMEA*, Quality Resources, 1996. ISBN: 0527763209.

8. Deliverables for Today:

Take-Home Assignment #4

9. Assignment for Next Time:

Take-home Assignment #5: Identify a critical infrastructure asset that you are somehow familiar with and use it to define a system. You may build on the results from your previous assignments, or construct a completely new system. For this system, conduct an FMEA and AFDA to uncover potential weaknesses in the system. What are the strengths of your analysis? What are the weaknesses of your analysis? How can your analysis be improved? Write 500 words addressing these three questions.

LESSON 6 TOPIC: LOGIC AND SYSTEMS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: binary; logic; failure; success; AND gate; OR gate; complement; Top Event; and basic event
- Discuss basic logical analysis, including AND, OR, and NOT (i.e. De’Morgan’s Laws)
- Construct a truth table corresponding to a simple fault tree
- Construct and analyze fault trees of simple systems

2. Rationale:

Prior to this lecture, learners were asked to reduce systems from a whole into its parts. However, little attention has been paid to formalizing how the parts of a system, or more specifically, how the workings of a part relate to the performance of the system. This lecture introduces fault tree analysis, a technique for describing a system in terms of how lower-level failures can lead to total system failure.

3. Discussion Questions:

- What is the difference between AND, OR, and NOT logic?
- What is the complement of failure?
- What is the difference between a fault tree and a success tree? Which do you prefer?
- How would you convert a fault/success tree into a success/fault tree?
- How would a fault tree be different if each event (basic event, top event) could take on one of more than two states?
- What is the right way to construct a fault tree of a system?
- Can you construct a fault tree from a truth table? What are some issues associated with this?

4. Class Agenda:

Activity	Duration
Presentations for Assignment #5	30 minutes
Discussion on fault tree analysis	45 minutes
Individual problems on fault tree analysis	20 minutes
Review of fault tree analysis problems	25 minutes
Fault Tree Analysis exercise	45 minutes
Debriefing on the exercise	15 minutes
Total	180 minutes

5. In-Class Activity: Individual Fault Tree Analysis Problems: The instructor will assign 10-20 fault tree analysis problems that ask learners to identify parts of a fault tree, identify single-point failures, interpret, and calculate top event probabilities for simple fault trees. The goal of this activity is to help learners build intuition for processing and

understanding fault trees.

Fault Tree Analysis Exercise: The instructor will provide learners with a reliability block diagram depicting an infrastructure system and/or a comprehensive description of a system. From here, learners will be asked to construct and interpret the corresponding fault trees for one or both of these systems. The goal of this activity is to provide an opportunity for learners to practice converting one system representation (i.e., block diagram or description) into the equivalent fault tree.

6. Required Reading:

H. Kumamoto, and E. J. Henley, “Probabilistic Risk Assessment and Management for Engineers and Scientists,” IEEE Press, 1996, 165-222.

National Aeronautics and Space Administration, *Fault Tree Handbook with Aerospace Applications*, 2002. Available at: <http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf>.

7. Additional Recommended Reading:

Nuclear Regulatory Commission, *Fault Tree Handbook*, NUREG-0492, 1981. Available at: <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf>.

R. V. Matalucci, “Risk Assessment Methodology for Dams (RAM-D),” *Proceedings of the Sixth International Conference on Probabilistic Safety Assessment and Management (PSAM6)*, 23–28 June 2002 San Juan, Puerto Rico, USA, Vol. 1, 2002, 169–176.

8. Deliverables for Today:

Take-Home Assignment #5

9. Assignment for Next Time:

Take-Home Assignment #6: Learners will be provided with several representations of different systems and will be asked to construct the corresponding fault trees and success trees. Learners will be asked to draw these trees using software such as MS Word, MS Visio, or OpenFTA (<http://www.openfta.com/>).

LESSON 7 TOPIC: ESTIMATING SYSTEM PERFORMANCE

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: performance; events; event trees; conditional logic; dependence; possibility trees; mutually exclusive; collectively exhaustive; sample space; Venn diagram; incident; and timeline
- Draw a Venn diagram depicting possible events within a sample space
- Apply event tree analysis to understand and describe how systems work

2. Rationale:

So far, methods discussed in class have not considered the temporal aspect of system performance. This lecture will introduce learners to the role that time plays in the evolution of events occurring within a system.

3. Discussion Questions:

- How does event tree analysis compare to fault tree analysis? What are the similarities? What are the differences?
- What is the purpose of an event tree? How are event trees the same or different than possibility trees?
- What is the difference between an event tree and a timeline?
- What role does conditional logic play in event tree/possibility tree analysis?
- Some argue that fault tree analysis and event tree analysis was created to deal with the problem of having a lack of data. Explain what you think they mean by this.
- What are some potential pitfalls associated with performing an event tree analysis? What are strengths of the method? Weaknesses?

4. Class Agenda:

Activity	Duration
Presentation of Assignment #6	30 minutes
Lecture and discussion about event trees	45 minutes
In-class Event Tree Analysis exercise	60 minutes
Debriefing and discussion	45 minutes
Total	180 minutes

5. In-Class Activity: Event Tree Analysis Exercise:

In this exercise, the instructor will provide learners with a narrative description of how a system works and how it can fail. This narrative description may be accompanied by an FMEA table or some other visual or tabular information. From this information, learners will be asked to construct an event tree that traces out all possible ways the system might fail over following exposure to some specified hazardous situation (e.g., explosion, earthquake, pipe failure, etc.). The goal of this assignment is to provide learners with practice working with mutually exclusive, collectively exhaustive possibilities of what can occur at different points along a timeline of system performance.

6. Required Reading:

M. E. Pate-Cornell, "Fault Trees vs. Event Trees in Reliability Analysis," *Risk Analysis*, 4(3), 1984, 177-186.

M. Rausand, "System Analysis: Event Tree Analysis," 2005. Available at: <http://www.ntnu.no/ross/srt/slides/eta.pdf>.

7. Additional Recommended Reading:

S. S. Epp, *Discrete Mathematics with Applications*, Brooks-Cole, 2010, 525-539.

8. Deliverables for Today:

Take-Home Assignment #6

9. Assignment for Next Time:

Systems Analysis Mid-Term Assignment

Assignment due in Two Weeks:

Take-Home Assignment #7: This assignment focuses on constructing an event tree associated with all possible events that may occur following the occurrence of a potentially catastrophic incident affecting an infrastructure facility. The instructor will provide the incident and some information about the particular asset and associated system that could be used to construct the event tree. The learner will construct the event tree and identify/describe all paths that lead toward an undesirable outcome.

LESSON 8 TOPIC: MID-SEMESTER REVIEW

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Evaluate recorded presentations of student work for clarity, coherence, and completeness
- Discuss selected topics/provide subject review as appropriate

2. Rationale:

Lesson 8 occurs at the halfway point of the semester. It is appropriate at this point for learners to present to the class their analysis of a real infrastructure system and discuss ways to further study the system to yield meaningful insights to support decision-making. Presentations will not be made live, but rather presented to the class as YouTube videos. The rationale for this is that preparing a YouTube video requires careful attention and preparation by the learner to produce a clear, concise, and complete summary of their analysis, and the experience of watching others listen to a particular learner's presentation will allow the student to see how the audience responds to his/her presentation.

3. Discussion Questions:

For each presentation:

- Is the system being presented fully or clearly described?
- What are the strengths of the analysis?
- What are the weaknesses of the analysis?
- What can be done to improve the analysis?

4. Class Agenda:

Activity	Duration
Presentation of mid-term assignments with group discussion	180 minutes
Total	180 minutes

5. Required Reading:

None

6. Additional Recommended Reading:

None

7. Deliverables for Today:

Mid-term project

8. Deliverables for Next Time:

Take-Home Assignment #7 (assigned during Lesson 7)

LESSON 9 TOPIC: QUANTIFYING SYSTEM PERFORMANCE

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: statistics; median; mean; standard deviation; mode; data; probability; complement; histogram; trendlines; and frequency
- Construct a data classification system for working with data
- Construct a chronology and a timeline showing a comprehensive history of events
- Summarize a data set using descriptive statistics, histograms, and trendlines

2. Rationale:

To this point, the emphasis in the class has been on methods for describing systems and reasoning about their performance. In this lecture, learners will become acquainted with working with historical data, organizing it, presenting it, and computing statistics with it.

3. Discussion Questions:

- What role does statistics play in systems analysis?
- What are some challenges with using statistics of past events to estimate the probability of future events?
- What are timelines and how are they useful?
- What is the difference between a chronology and a timeline?
- What is the purpose of a data classification system?
- How are timelines different from event trees?
- Consider the statement “it is impossible to quantify things when it comes to security.” Do you agree or disagree with this statement?

4. Class Agenda:

Activity	Duration
Discussion of Take-Home Assignment #7	30 minutes
Lecture on data classification, chronologies	30 minutes
Data classification exercise	30 minutes
Lecture on descriptive statistics	30 minutes
Descriptive statistics exercise	30 minutes
Debriefing	30 minutes
Total	180 minutes

5. In-Class Activity: Data Classification Exercise: The instructor will provide learners with a data set describing incidents that affected infrastructure or other systems over the past 10-20 years. In this exercise, learners will construct a data classification system aimed at providing insights into the types of events that occurred, what sectors were affected, etc. Afterward, learners will construct a chronology and timeline of the events broken up according to criteria specified by the instructor.

Descriptive statistics exercise: In this exercise, learners will summarize the data classification system and sorted data from the previous exercise using descriptive statistics, histograms, and trendlines. If computers are available, this can be done in Excel. If not, this can be done using graph paper and pencil.

6. Required Reading:

M. D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, Crown Business, 1998, 87-93.

J. K. Clauser and S. M. Weir, *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*, Defense Intelligence School, 1976, 194-209 and 211-243.

7. Additional Recommended Reading:

P. E. Pfeiffer and D. A. Schum, *An Introduction to Applied Probability*, Academic Press, 1973.

R. H. Morneau and G. E. Morneau, *Security Administration: A Quantitative Handbook*, Butterworth-Heinemann, 1982.

8. Deliverables for Today:

Take-Home Assignment #7

9. Assignment for Next Time:

Take-Home Assignment #8: In this assignment, learners will be provided with a second data set that is different from the one used in class. Using this data, learners will develop a data classification system oriented toward a particular question or theme specified by the instructor, construct a chronology or timeline, and summarize the data using simple statistical tools.

LESSON 10 TOPIC: THREATS TO SYSTEMS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: threat; convergent thinking; divergent thinking; and brainstorming
- Apply suitable brainstorming techniques such as Divergent-Convergent Thinking to construct sets of plausible threat scenarios

2. Rationale:

At this point, learners will start to focus on what can happen to a system that would cause it to suffer damage. The aim of this lecture is to introduce a technique aimed at encouraging creative thinking about plausible system threats.

3. Discussion Questions:

- What is meant by the phrase “failure of imagination”? How does this phrase apply to systems analysis?
- To what extent does divergent-convergent thinking mitigate “failure of imagination”?
- What are the strengths, weaknesses, and limitations of divergent-convergent thinking?
- Is divergent-convergent thinking a suitable technique for use in systems analysis? Can it be applied elsewhere other than for threat analysis?

4. Class Agenda:

Activity	Duration
Discuss Take-Home Assignment #9	30 minutes
Lecture on brainstorming, threat analysis	45 minutes
Divergent-Convergent Thinking exercise	75 minutes
Debriefing	30 minutes
Total	180 minutes

5. In-Class Activity: Divergent-Convergent Thinking Exercise:

In this exercise, learners will consider a particular system and will be asked to generate a representative list of plausible threats with the potential to compromise the system. Learners will work in groups and apply the Divergent-Convergent Technique to develop a list of scenarios. For each scenario, learners will employ their knowledge of the system to fully explain how the threat could cause harm.

6. Required Reading:

M. D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, Crown Business, 1998, 80-86.

E. G. Bitzer and R. Johnston, “Creative Adversarial Vulnerability Assessments,” *Journal of Physical Security*, 2 (1), paper 5, 2007. Available at: <http://jps.anl.gov/vol.2/5->

[Creative Assessments.pdf](#).

7. Additional Recommended Reading:

National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 2004. Available at: <http://www.9-11commission.gov/report/911Report.pdf>.

J. O. Matschulat, "An Introduction to the Concept and Management of Risk," in Johnson, T. A. ed. *National Security Issues in Science, Law and Technology*, CRC Press, 2005, 291-357.

8. Deliverables for Today:

Take-Home Assignment #8

9. Assignment for Next Time:

No assignment due next time

LESSON 11 TOPIC: IMPACTS OF SYSTEM INCIDENTS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: utility; stakeholders; criterion; and weighting factor
- Apply the Weighted Ranking method to estimate the level of concern or impact that would be associated with a variety of disruptive situations
- Compare the Weighted Ranking method to the Analytic Hierarchy Process (AHP)

2. Rationale:

This lecture returns to the constructivist view of systems to consider the impact that disruption or changes in infrastructure system performance affects stakeholders.

3. Discussion Questions:

- What is the relationship between security context and utility?
- What is the connection between the Weighted Ranking method and the constructivist view of systems?
- How does the Weighted Ranking Method and AHP compare? What are the strengths, weaknesses, and limitations of each?
- What role does Pairwise Ranking play in estimating the potential impact of system incidents?

4. Class Agenda:

Activity	Duration
Recap of previous 10 lectures	30 minutes
Lecture on decision making techniques	30 minutes
Weight Ranking and AHP Exercise	90 minutes
Debriefing and discussion	30 minutes
Total	180 minutes

5. In-Class Activity:

Weighted Ranking and AHP Exercise: In this exercise, learners will consider a particular system and will be asked to evaluate the significance or impacts of alternative end states following a system incident. This exercise is rather lengthy because it may require learners to describe a system, identify potential threats to the system using various brainstorming techniques, construct an event tree for one or more of these events, and then appraise the outcomes from each branch of the tree using either the Weighted Ranking method or the AHP.

6. Required Reading:

M. D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, Crown Business, 1998, 246-281.

T. L. Saaty, "Decision Making with the Analytic Hierarchy Process," *International Journal of Services Sciences*, 1 (1), 2008, 83-98.

Concordia University, "Pairwise Ranking," Part of the *Coast Guard Process Improvement Guide*, 2011. Available at: <http://web2.concordia.ca/Quality/tools/18pairwise.pdf>.

7. Additional Recommended Reading:

J. S. Hammond, R. L. Keeney, and H. Raiffa, *Smart Choices: A Practical Guide to Making Better Decisions*, Crown Business, 2002.

R. T. Clemen, *Making Hard Decisions: An Introduction to Decision Analysis*, South-Western College Publishers, 1997.

8. Deliverables for Today:

No assignment due today

9. Assignment for Next Time:

Take-Home Assignment #9: In this assignment, learners will consider a system that they are familiar with, either from experience or from previous assignments. Here, the learner will be asked to further consider how a particular incident afflicting the system could evolve over time, and develop a complete set of end states (scenarios). Learners will then rank order these scenarios using each of the following techniques based on the level of concern: (a) intuition; (b) Pairwise Ranking; (c) Weighted Ranking; and (d) the Analytic Hierarchy Process.

LESSON 12 TOPIC: PROTECTING SYSTEMS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: protection and decision
- Apply the pros/cons/fixes technique to evaluate the merits and demerits of alternative risk management strategies

2. Rationale:

At this point in the semester, learners are well versed in various techniques used for understanding systems. It should seem straightforward now that much of the insight generated with these tools can be used to identify ways to improve system performance or protect against a variety of threats. This lecture presents a simple technique for performing an approximate analysis of alternative protection options.

3. Discussion Questions:

- How do the results of analysis methods such as FMEA, AFDA, fault tree analysis, and event tree analysis assist with identifying alternative protection strategies for a system?
- What are the strengths of the Pros/Cons/Fixes method? What are its weaknesses?
- What are some alternative methods? How are they better or worse?
- What types of information is needed to complete a Pros/Cons/Fixes analysis?

4. Class Agenda:

Activity	Duration
Discussion of Take-Home Assignment #11	30 minutes
Lecture on pros/cons/fixes	30 minutes
Pros/Cons/Fixes Exercise	60 minutes
Debriefing	30 minutes
Discussion of alternative decision analysis tools	30 minutes
Total	180 minutes

5. In-Class Activity: Pros/Cons/Fixes Exercise

In this exercise, learners will consider a system that they have studied at sometime during the course of the semester. This time, they will use the insights gained in their study to identify alternative ways to either improve the performance of the system or better protect the system against potential threats. For each alternative, learners will apply the Pros/Cons/Fixes technique to evaluate the relative merits and demerits of each.

6. Required Reading:

M. D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, Crown Business, 1998, 72-79.

Benjamin Franklin, "Letter to Joseph Priestly," Dated September 19, 1772. Available at: <http://www.procon.org/view.background-resource.php?resourceID=1474>.

7. Additional Recommended Reading:

R. L. Keeney, *Value Focused Thinking: A Path to Creative Decisionmaking*, Harvard University Press. 1996.

8. Deliverables for Today:

Take-Home Assignment #9

9. Assignment for Next Time:

No assignment due next time

LESSON 13 TOPIC: MONITORING SYSTEM PERFORMANCE

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Define the following terms: indicators and warnings
- Develop a set of measurable indicators of systems performance
- Apply the Indicators and Signposts of Change methodology to track system performance over time

2. Rationale:

To this point in the semester, our focus has been on systems as they are with some consideration paid to estimates of system performance under stress. In this lecture, we consider techniques for measuring system performance over time.

3. Discussion Questions:

- What is the connection between state variables and indicators?
- What types of indicators would you look for to measure the performance of the electric power grid? Water distribution system? Traffic?
- How can the Indicators and Signposts of Change methodology be used to inform decisions to issue warnings to decision-makers?
- How many metrics are typically needed to answer questions of interest to decision makers? When is one metric enough? Is one metric ever enough?

4. Class Agenda:

Activity	Duration
Discussion of Take-Home Assignment #12	30 minutes
Lecture/discussion on indications and warning analysis	45 minutes
Measure Development Exercise	30 minutes
Debriefing	30 minutes
Total	180 minutes

5. In-Class Activity: Measure Development Exercise

In this exercise, learners will be asked to propose and describe metrics used for understanding and tracking the performance of a particular critical infrastructure system, subsystem, or asset over time. Afterward, learners will develop a strategy for collecting data to assign values to these metrics and discuss data quality issues. The goal of this assignment is to provide learners with an experience developing measures that can be used to evaluate the present condition of a system.

6. Required Reading:

Central Intelligence Agency, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, 2005. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.

D. W. Hubbard, *How to Measure Anything: Finding the Value of Intangibles in Business*, Wiley, 2nd Ed., 2010.

7. Additional Recommended Reading:

R. K. Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable," *World Politics*, 23, 1979. Available at: <http://www.foia.cia.gov/CzechInvasion/8-StrategicWarning/1979-09-01.pdf>.

8. Deliverables for Today:

No assignment due

9. Assignment for Next Time:

No assignment due next time

LESSON 14 TOPIC: SYSTEM EVOLUTION AND REVIEW

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Apply future forecasting techniques to anticipate how different infrastructures will evolve over time and why
- Summarize the entire systems analysis course and discuss how each lecture relates to the topic of systems analysis
- Verbally describe “systems analysis” in two minutes or less

2. Rationale:

This final lecture emphasizes the importance of taking a forward-looking view regarding how infrastructure, and systems in general, evolves over time. In addition, this lecture will attempt to tie together all topics in this course into a coherent whole.

3. Discussion Questions:

- How do you expect threats and vulnerabilities to evolve over time?
- What are some significant drivers of change?
- What is the difference between a prediction and an estimate? Which are more useful? Which are easier to obtain?
- Is it important to study infrastructure evolution?
- How does such study tie in with risk management in general?
- How can any particular conception change over time?

4. Class Agenda:

Activity	Duration
Discussion of final projects	30 minutes
Lecture on technology evolution	45 minutes
Technology Forecasting exercise	45 minutes
Discussion and course wrap-up	60 minutes
Total	180 minutes

5. In-Class Activity: Technology Forecasting Exercise

In this exercise, learners will be assigned to study an infrastructure sector they are familiar with and will be asked to apply one or more future forecasting techniques to explore alternative ways the sector can evolve over time. Special attention will be paid to how new vulnerabilities emerge over time, and what threats may rise to create new risks. The goal of this exercise is to not come up with absolute predictions, but to describe the range of plausible futures and how they impact any assessment of risk.

6. Required Reading:

Central Intelligence Agency, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, 2005. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.

T. J. Gordon, "Cross-Impact Method," 1994. Available at: [http://www1.ximb.ac.in/users/fac/dpdash/dpdash.nsf/23e5e39594c064ee852564ae004fa010/2a7a6240bcf05ebde5256906000a7322/\\$FILE/Cross-im.pdf](http://www1.ximb.ac.in/users/fac/dpdash/dpdash.nsf/23e5e39594c064ee852564ae004fa010/2a7a6240bcf05ebde5256906000a7322/$FILE/Cross-im.pdf).

National Research Council, *Avoiding Surprise in an Era of Global Technology Advances*, 2005. Available at: http://www.nap.edu/catalog.php?record_id=11286.

7. Additional Recommended Reading:

None

8. Deliverables for Today:

No assignment due

9. Assignment for Next Time:

Final Course Project (due at time of instructor's choosing)

LESSON 15 TOPIC: FINAL PRESENTATIONS

1. Lesson Goals/Objectives:

At the end of this lecture, learners will be able to:

- Provide constructive feedback to peers on the quality of their work

2. Rationale:

This final session emphasizes learner presentations of final course projects. This experience should help learners tie all course content together by considering the myriad systems studies by others.

3. Discussion Questions:

- Do any of the presentations seem to deviate from what you consider to be sound systems analysis?
- Which of the presentations/analyses are examples of good systems analysis?
- How could the presentations/analyses be improved?

4. Class Agenda:

Activity	Duration
Class presentations	180 minutes
Total	180 minutes

5. In-Class Activity:

None

6. Required Reading:

None

7. Additional Recommended Reading:

None

8. Deliverables for Today:

Final Course Project (due at time of instructor's choosing)