Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Preparing the next generation of SE students for a brave new world: Making the case for an early introduction of ISSE

Susan Hansche, CISSP, ISSEP

Abstract: The main thesis of this paper is that Information Systems Security Engineering (ISSE) should be an essential element of introductory Systems Engineering (SE) courses. Based on a small informal survey, ISSE concepts seem not to be included in SE introductory courses. This paper, therefore, makes the argument that security learning objectives need to be integrated into the initial stages of teaching SE students. In the process of exploring whether SE students are properly exposed to ISSE, this paper reviews a current introductory SE course description and its learning objectives, provides sample security learning objectives, reviews the IEEE SE model, and finally suggests the Information Assurance Technical Framework (IATF) as one way of including security into SE models.

Index terms – Information Assurance, Infrastructure Assurance

I. Introduction

Systems engineering is a subject that has developed relatively recently and covers the mathematical modeling, design, and analysis of systems. As an academic endeavor, this field concentrates on how different components in a system fit together and how to ensure that the system is designed in such a manner that all components interact together in an efficient way. The International Council of System Engineering (INCOSE) defines systems engineering as "An interdisciplinary approach and means to enable the realization of successful systems."[1]

Systems Engineering education and training courses typically focus on the knowledge and skills necessary to understand the analysis and design of complete engineering systems. More recently, academic and training courses have added a specific concentration in the analysis and design of complex and distributed information systems and software engineering for such systems. Should the next step in this evolutionary process be a spotlight on adding security objectives to the core topics?

The purpose of this paper is to outline what is currently taught in basic Systems Engineering (SE) type courses (whether it is in a training or academic environment) and also to discuss whether security objectives can be included as part of the learning objectives and lesson topics. This presumes, of course, that introductory SE courses explore the activities of a common SE model. In order to do this, the paper is divided into four topic areas:

- Sample objectives from a SE course. In this section the description and learning objectives from an introduction information systems SE course is provided.
- Adding Security Learning Objectives. The information systems of today and tomorrow demand security. Thus, there is a need for security learning objectives. Some sample security learning objectives are provided as examples of what could be added to SE courses.
- The IEEE SE Model. The basis for a generic SE model is taken from the Institute of Electrical and Electronics Engineers (IEEE) Standard 1220-1998 "IEEE Standard for Application and Management of the Systems Engineering Process."
- The Information Assurance Technical Framework (IATF) Information Systems Security Engineering (ISSE) Model. Exploration of whether the IATF model for adding security to a typical SE model is appropriate for learning objectives and topics.

This paper is not discussing the work being performed at various universities through the National Security Agency's Centers for Excellence in Information

---

Ms. Hansche is the training director for information assurance at PEC Solutions in Fairfax, Virginia. She is the lead author of "The Official (ISC)² Guide to the CISSP Exam," which is a reference for professionals in the information system security field studying for the Certified Information Systems Security Professional (CISSP) exam. Her second book "Information Systems Security Engineering: A Handbook for the ISSEP" will be released Fall 2004. This book explores the ISSE concepts in greater detail.

Ms. Hansche has been working as the contractor program manager of information assurance training for the U.S. Department of State since 1998. In this role, she has taught (and learned from) numerous engineers the fundamental elements and core concepts of information system security. She can be reached via email at: susan.hansche@pec.com

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Assurance. Indeed, these university programs have focused on integrating security into various curricula. From a brief initial review, these information assurance curricula seem to consist of customized courses within information technology, computer science, or software engineering programs and are not presented in SE curriculums. While I have not conducted an extensive survey of all relevant SE academic programs, security objectives do not appear to be included in most introductory SE courses.

Let us begin by reviewing sample objectives from an introductory SE course. The point of this exercise is to show that security learning objectives are not included in the course description nor in the goals listed in the course syllabus.

II. Sample Objectives from an Introductory SE Course

My brief sampling of learning objectives for introductory SE courses is from ten SE programs that have listed their course descriptions and/or objectives on their websites. Although this can by no means be considered comprehensive data, it does provide a sample of the type of introductory SE course descriptions and objectives. (Appendix A provides all ten examples.)

Note that of this small sample, only one program's introductory SE course mentioned security. Massachusetts Institute of Technology (MIT) Spring 2004 offering of Computer System Engineering describes the course as "Topics on the engineering of computer software and hardware systems: techniques for controlling complexity; strong modularity using client-server design, virtual memory, and threads; networks; atomicity and coordination of parallel activities; recovery and reliability; privacy, security, and encryption; and impact of computer systems on society." [2]

Of the nine other universities, this specific example is from Portland State University; course *SYSE 591 Systems Engineering Approach*. The course description: "Engineering of complex hardware, software systems encompasses quantitative methods to understand vague problem statements, determine what a proposed product/system must do (functionality), generate measurable requirements, decide how to select the most appropriate solution design, integrate the hardware and software subsystems and test the finished product to verify it satisfies the documented requirements. Additional topics that span the entire product life cycle include interface management and control, risk management, tailing of process to meet organizational and project environments, configuration management, test strategies and trade-off studies."[3]

The SYSE 591 course syllabus lists the specific goals and objectives as:

- "Understand systems engineering as an interdisciplinary process and show its relationship to traditional engineering disciplines, applied science and program management.
- Demonstrate its value in the development of products, processes, and services.
- Explain fundamental concepts such as defining internal/external customer's needs early in the development cycle, generating requirements, selecting alternative solutions, testing and measuring of solution development relative to requirements.
- Access case studies, templates, and checklists that support the systems engineering approach.
- Tailor the general Systems Engineering Management Plan to the unique requirements of a specific organization and project.
- Utilize automated tools for report writing, tracking of requirements, capturing solution alternatives (e.g., trade studies), performance, cost, and scheduling.
- Apply basic risk analysis and management techniques to product development.
- Form and maintain successful interdisciplinary and cross-functional teams.
- Apply standards (ISO, EIA, and IEEE), the SEI Capability Maturity Models - Integration (CMM - I) throughout the development process." [4]

Absent from the SYSE 591 course description and goals are the security objectives. You may ask if the SE studying information systems needs to understand the concepts of security. Since network systems today are more complex and interconnected, they require a new way of thinking that includes security. Thus, I believe it is important for the SE student to not only grasp security concepts, but also to appreciate the importance of security. Moreover, as I will point out in the next topic, is the importance of providing this information early in the student's education.

III. Adding Security Learning Objectives

Today's distributed information systems operate in an environment where connections to other entities and/or the Internet are required. This expansion of internetworking or interconnectedness of computer systems has evolved into a global integrated distributed network with worldwide users. The availability of information to users continues to grow so that at any time, users have access to the information they need. The only mechanisms to control how users access information are the security controls that are implemented.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Today, and especially tomorrow's systems will require the SE (that is the engineer that defines, designs, and develops information systems) to have a new and expanding knowledge of the role and importance of security. As a member of an engineering team that is responsible for designing systems, a SE needs to understand security needs, security risks, security constraints, and how to design a system with security as one of the primary focuses.

Typically, security is thought of only after the system has been designed. There is a problem with this though, when security is added to a system as an afterthought it can create resource issues, such as increased costs and possible functional degradation. Thus, adding security to a system after it is developed is not the best approach. Similarly, educating the SE student about security at an advanced stage of his or her academic development does not create the same awareness and importance of this issue. If students are given a sense of the significance (and consequences) of security at the outset (i.e., in introductory courses) they will have a greater understanding of how security issues and concerns fit into engineering activities. Essentially, including security objectives only later in the curriculum does not fully integrate security into the thinking and design processes of tomorrow's SE professionals. In order to create secure systems that operate in complex and interconnected environments, an SE needs to understand the importance of security from the beginning –thus, security should be included in introductory courses.

Security-related learning objectives can be written in various forms. To provide some discussion and possible ideas, here is a sample of information system security objectives:

- Understand the importance of security when using system-engineering principles to define, design, develop, implement, verify, and maintain information systems.
- Identify the security needs and requirements of an information system project.
- Identify the security constraints and impact it may have on the security architecture.
- Identify the security solutions that will meet the identified security needs/requirements and document it in the security architecture.
- Determine how the system security solutions should be configured, enabled, tested, and verified.
- Define the assurance mechanisms needs to ensure that the implemented security solutions have met the security needs.

Obviously, these are just examples of security lesson objectives and each course designer/instructor would create their own lesson objectives based on the curriculum needs. Regardless of how the objectives are written, the goal is to include security as part of the learning process.

The next topic focuses on how these security objectives can be included into a basic SE model. As a reference point, a brief review of the fundamental concepts of the international standard for systems engineering is provided.

IV. The IEEE Systems Engineering Model

IEEE Standard 1220-1998 "IEEE Standard for Application and Management of the Systems Engineering Process" defines the objective for systems engineering as "…to provide high-quality products and services, with the correct people and performance features, at an affordable price, and on time. This involves developing, producing, testing, and supporting an integrated set of products (hardware, software, people, data, facilities, and material) and processes (services and techniques) that is acceptable to customers, satisfies enterprise and external constraints, and considers and defines the processes for developing, producing, testing, handling, operating, and supporting the products and life cycle processes. This objective is achieved by simultaneous treatment of product and process content to focus project resources and design decisions for the establishment of an effective system design. This involves an integrated handling of all elements of a system, including those related to manufacturing, test, distribution, operations, support, training, and disposal." [5]

IEEE 1220 is intended to guide the development of systems, including computers and software, for commercial, government, military, and space applications. It applies to an enterprise within an organization that is responsible for developing a product design and establishing the life-cycle infrastructure needed throughout the product's life cycle.

A key component of IEEE 1220 is its interdisciplinary approach to developing systems. The standard defines the tasks that are required throughout a system's life cycle to transform customer needs, requirements, and constraints into a system solution. These core concepts – needs, requirements, and constraints – will also be seen in the ISSE model, except they will appear as security needs, security requirements, and constraints that affect those security needs and requirements.

IEEE 1220 is important because it defines the non-security phases and activities of the SE process for components and systems. These SE phases can be seen in the ISSE model defined by IATF. The difference is that in the ISSE model, security is integrated into each of the

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

phases. The next topic provides a brief introduction to the ISSE model.

V. The Information Assurance Technical Framework (IATF) Information Systems Security Engineering (ISSE) Model

In response to the emerging demands for greater United States Government (USG) information system security capabilities, the National Security Agency's (NSA) Information Systems Security Organization (NSA ISSO) instituted a Systems Security Engineering Process Action Team (SSE PAT) in mid-1993. The mission of the SSE PAT was to synthesize previous and new information systems security initiatives into a consistent, customer-focused model for ISSE, which is intended as a discipline of systems engineering. Although the ISSE process can be tailored to any organization, the design is intended and focused on following USG standards and directives for system acquisition, system life cycle, system components, system certification and accreditation, etc. [6]

Essentially, ISSE is the functional application of processes for the design, development, and operation of efficient, economical, and secure networks for the communication of information/knowledge. To meet the security requirements, the process must account for the primary security services: availability, integrity, confidentiality, authentication, and non-repudiation.

A central element of the ISSE model is to first understand the security needs of the organization in relationship to the security services. As important as it is to comprehend the security needs of the organization, it is also important to understand the security objectives of the system based upon the organization. For example, organizations processing national security information would require stricter security objectives. An additional element of the ISSE methodology is to design and develop a system in such a manner that it can safely resist the forces to which it may be subjected. Recognizing this critical element, an encompassing ISSE definition could be stated as:

> "ISSE is the art and science of discovering the users security needs and the overall security needs of the organization; designing and developing, with economy and elegance, an information system that ensures an appropriate level of availability, integrity, confidentiality, authentication, and non-repudiation which are based upon valid risk management decisions; and the system can safely resist the forces to which it may be subjected."

The IATF is supported by the Information Assurance Technical Framework Forum (IATFF), which is an NSA sponsored outreach activity created to foster dialog amongst USG agencies, U.S. Industry, and U.S. Academia who provide their customers solutions for information assurance problems. According to IATFF, "the ultimate objective of the IATFF is to agree on a framework for information assurance solutions that meet customers' needs and foster the development and use of solutions that are compatible with the framework." [7]

The IATF ISSE model is one option for instructors/course designers to use when including security-learning objectives in SE courses. ISSE is defined as a "discipline of systems engineering that supports the evolution and verification of an integrated and life cycle balanced set of system product and process solutions that will satisfy a customer's information security needs. The focus of the process is to identify security risks and to subsequently minimize or contain those risks." [8]

In today's ISSE environment, an ISSE practitioner is faced with a range of tools and techniques that can be utilized for any given design problem. Under the guidance of subject matter experts, the IATF ISSE framework was developed to standardize an information systems security process model that would follow the design of SE principles, but would also emphasize the role of security in designing and developing information systems.

The IATF identifies a generic SE model as six activities that are also the basic activities of the ISSE process. These are:

- Discover Needs
- Define System Requirements
- Design System Architecture
- Develop Detailed Design
- Implement System
- Assess Effectiveness

The difference is the IATF ISSE model incorporates security into the fundamental SE activities. Based on IATF, Chapter 3, the activities in the ISSE model are:

1. Discover information protection needs. Ascertain why the system needs to be built, what needs the system must fulfill, and what system resources need to be protected and at what level.
2. Define system security requirements. Define the system in terms of not only what the system needs to be able to do, but also what security is required to meet the information protection needs.
3. Define system security architecture. Using previously documented information, choose the types of security components that will perform specific security functions. This process is the core of designing the security architecture.
4. Develop detailed security design. Based on the security architecture, begin to design the security

features of the system to be able to do what is needed.

5. Implement system security. Build/implement the security function(s) of the system so it does what it is intended to do.
6. Assess security effectiveness. Assess the degree to which the system, as it is defined, designed, and implemented, meets the security needs of the organization. This assessment activity occurs during and with all the other activities in the ISSE process. [9]

Table 1 [10] provides details on the differences between SE activities and ISSE activities in the life-cycle model. In some life-cycle models, each element is considered a step of the process. The ISSE model does not consider the elements as steps, but rather as activities. This is because the use of the word *step* indicates some type of hierarchical movement from one place to another.

The ISSE model views the activities as a holistic entity, not a timeline where one activity needs to be completed before the other. Instead, each activity must be considered in relationship to another activity. For example, in order to adequately discover the information protection needs, it is necessary to also understand the organization's system security requirements.

The IATF is just one model that could form the basis for including security learning objectives and topics. One of the reasons why is it helpful is the correlation it provides between the basic SE activities and the ISSE activities. Another option for the SE field is to use the INCOSE Systems Engineering Centers of Excellence (SECOE) research agenda as a tool for exploring and designing other security models that can be included in SE courses. [11] Appendix B provides a brief summary of the INCOSE SECOE.

VI. SUMMARY

Due to the complexity and interconnectedness of information systems today, those responsible for defining, architecting, designing, developing, and constructing systems need to be aware of how security fits into such activities. The need for and awareness of secure systems is increasing exponentially. In this brave new world, SEs will become a first line of defense in protecting our information systems and the information they process. Securing systems has therefore, I believe, become priority number one. Thus, today's educators need to be aware of how to focus their course learning objectives to include security, and to expose SE students to security objectives from the start of their academic careers.

With a review of limited syllabi, it would appear that security objectives are not included as an integral aspect of introductory SE courses. In this paper, an example of a course description and learning objectives from an introductory SE course was provided, noting that it did not include security as a learning objective or topic. [Please refer to Appendix A for other sample SE course descriptions and learning objectives.] A list of possible security learning objectives was included so instructors and professors teaching SE can begin to look at how to include security concepts within a SE model. In addition, the IATF provides a framework for comparing SE and ISSE activities and how the two should be integrated.

Let me repeat the premise of this paper as a question: is it time for introductory educational (and training) SE courses to integrate security into their core learning objectives so that every SE student will have a minimum level of understanding of security and its importance to the design and development of information systems?

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Table 1 Corresponding SE and ISSE Activities [9]

SE Activities	ISSE Activities
Discover Needs The SE helps the customer understand and document the information management needs that support the business or mission. Statements about information needs may be captured in an information management model (IMM).	**Discover Information Protection Needs** The ISSE helps the customer understand the information protection needs that support the mission or business. Statements about information protection needs may be captured in an Information Protection Policy (IPP).
Define System Requirements The SE allocates identified needs to systems. A system context is developed to identify the system environment and to show the allocation of system functions to that environment. A preliminary system Concept of Operations (CONOPS) is written to describe operational aspects of the candidate system (or systems). Baseline requirements are established.	**Define System Security Requirements** The ISSE allocates information protection needs to systems. A system security context, a preliminary system security CONOPS, and baseline security requirements are developed.
Design System Architecture The SE performs functional analysis and allocation by analyzing candidate architectures, allocating requirements, and selecting mechanisms. The systems engineer identifies components or elements, allocates functions to those elements, and describes the relationships between the elements.	**Design System Security Architecture** The ISSE works with the systems engineer in the areas of functional analysis and allocation by analyzing candidate architectures, allocating security services, and selecting security mechanisms. The information systems security engineer identifies components or elements, allocates security functions to those elements, and describes the relationships between the elements.
Develop Detailed Design The SE analyzes design constraints, analyzes trade-offs, does detailed system design, and considers life-cycle support. The systems engineer traces all of the system requirements to the elements until all are addressed. The final detailed design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.	**Develop Detailed Security Design** The ISSE analyzes design constraints, analyzes trade-offs, does detailed system and security design, and considers life-cycle support. The information systems security engineer traces all of the system security requirements to the elements until all are addressed. The final detailed security design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.
Implement System The SE moves the system from specifications to the tangible. The main activities are acquisition, integration, configuration, testing, documentation, and training. Components are tested and evaluated to ensure that they meet the specifications. After successful testing, the individual components—hardware, software, and firmware—are integrated, properly configured, and tested as a system.	**Implement System Security** The ISSE participates in a multidisciplinary examination of all system issues and provides inputs to C&A process activities, such as verification that the system as implemented protects against the threats identified in the original threat assessment; tracking of information protection assurance mechanisms related to system implementation and testing practices; and providing inputs to system life-cycle support plans, operational procedures, and maintenance training materials.
Assess Effectiveness The results of each activity are evaluated to ensure that the system will meet the users' needs by performing the required functions to the required quality standard in the intended environment. The systems engineer examines how well the system meets the needs of the mission.	**Assess Information Protection Effectiveness** The ISSE focuses on the effectiveness of the information protection—whether the system can provide the confidentiality, integrity, availability, authentication, and nonrepudiation for the information it is processing that is required for mission success.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Appendix A

1. United States Naval Academy

ES 402: Systems Engineering Design
Course Description: "Introduction to the macro-techniques of engineering design including performance, reliability, management control, redundancy, man-machine systems and testing techniques. Design, construction, test and evaluation of an approved project is accomplished in the lab." The goals are defined as:

1. To demonstrate the interdisciplinary nature of the design function in Systems Engineering.
2. To examine in detail the components used in designing control systems including signal comparison, power amplification, and interfacing.
3. To provide broad Systems Engineering design concepts such as human engineering, reliability, economics, and ethics.
4. To provide practical experience in the design, construction, testing, and analysis of a design project proposed by the student and the oral and written communication of the results.

http://wseweb.ew.usna.edu/wse/systems/Courses/es402.htm

2. George Mason University

SYST 101 Understanding Systems Engineering
This course introduces students to the profession of systems engineering and the curriculum for a B.S. in Systems Engineering at George Mason University. The students will be introduced to large and small systems and asked to understand these systems through the provision of some hands-on experiences. . Key concepts will include the understanding of the requirements for a system and the translation of system-level requirements to component-level requirements. Several different kinds of example systems will be presented and discussed, specifically, what objectives of the system are, the system's major components, how the system works, and what some of the major design issues are. Each student will give a similar presentation on a system of the student's choice. Students working in groups will design, develop and test a system, and give an oral presentation to the class on the system they developed. The students will be responsible for writing several short papers on the curriculum and the presentations that they have heard.

SYST 430 Integration of Hardware and Software
Introduction to hardware and software components of computer systems. Study of hardware and software interchangeability. Understanding and analysis of factors that impact the effectiveness and efficiency of hardware and software integration. Topics include engineering fundamentals for computer design, hardware and software components, tradeoff between hardware and software, analysis of data representations and addressing, impact of the operation design and flow control design on the performance of computer systems, global control, operating system, memory management, input/output characteristics, bus systems, and efficiency analysis. Macro engineering of computer systems. Study of practical examples in the area of hardware and software design and development in the information technology industry.
http://www.gmu.edu/departments/seor/courses/syst-undergrad-courses.html

3. University of Virginia

SYS 201 - Systems Engineering Concepts
Three major dimensions of systems engineering will be discussed and their efficacy be demonstrated through case studies or examples. (1) The philosophy, art, and science upon which systems engineering is grounded, including guiding principles and steps in systems engineering. (2) The building blocks of mathematical models and the centrality of the state variables in systems modeling, including: State variables, decision variables, random variables, exogenous variables, inputs and outputs, objective functions, constraints; 3) Models, methods and tools in systems modeling, including: Project requirements, specifications, and management, linear models, discreet dynamic state equations, multiple objectives in systems engineering, decision making, and in management, hierarchical holographic modeling (HHM), influence diagrams, multiple objective decision trees (as a multistage modeling tool), dynamic programming (as a multistage modeling tool), probabilistic modeling and systems management. Case studies will supplement and complement the lectures.
http://www.virginia.edu/registrar/records/ugradrec//chapter10/chapter10-3.htm

4. University of Arizona, Department of Systems & Industrial Engineering

SIE 250/260 - Introduction to Systems and Industrial Engineering
Designation: Required course in systems and industrial engineering programs 2003-04 catalog description: Introduction to Systems and Industrial Engineering (3 units)
Description: Introduction to the methods that SIE people use when designing and operating systems. The focus is the early steps of the design process and includes defining the need and problem, formulating requirements, developing criteria and constraints, modeling the system, and analyzing system output. We will consider a variety of techniques and problem areas that may include systems modeling and simulation, linear program modeling, facility layout, production planning, control quality control, and human factors. Applications and case studies

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

from the engineering experience of the instructor will be used extensively.

Course objectives: This course is intended to give students background in the types of problems that SIE people work and the methods used to solve problems and design systems. We will place systems and industrial engineering in the engineering design process and go over examples throughout the semester. Our focus will be on the first 6 steps of the design process, need - problem - search - criteria and constraints - alternatives - analysis. We will consider techniques and problem areas such as CAD, facility layout, production control, system design and modeling, quality control, and human factors.
The class has the following specific educational goals for students. By the end of the course, the students should:

Understand the system design process including requirements development and system specifications.
- Ability to state the steps in the system design process
- Ability to take a system and define components, relationships, objectives, and constraints
- Ability to determine and state the requirements for a system

Understand the role of models in the system design process
- Ability to understand the difference between a model and the actual system
- Ability to determine objectives for a system based on user inputs
- Ability to use model output to help make decisions for system design

Understand and use standard SIE tools and vocabulary.
- Ability to construct drawings using AUTOCAD
- Ability to construct and analyze system simulation models using ITHINK
- Ability to construct and interpret simple X bar and R bar control charts
- Ability to use the "Solver" feature in MSExcel to optimize functions subject to constraints
- Ability to define and converse with SIE terms such as supply chain management, facility layout, requirements management, criteria and constraints, design process

To gain experience working in teams to develop solutions to complex engineering design problems.
- Ability to take on the different roles of a team (leader, scribe, member)
- Ability to understand the worth of all team members and to be able to see how diversity is valuable

To gain experience writing professional quality reports.
- Ability to construct reports for case studies that include documenting functional requirements, describing modeling approaches, stating results, and discussing sensitivity analyses.

http://www.sie.arizona.edu/course_pages/

5. Portland State University

SYSE 591: Systems Engineering Approach
Course Description: This course provides the knowledge and skills necessary to plan, organize, perform, control, and verify the engineering of complex hardware, software systems. The student will gain interdisciplinary knowledge concerning methods to understand vague problem statements, determine what a proposed product/system must do (functionality), generate measurable requirements, decide how to select the most appropriate solution design, integrate the hardware and software subsystems and test the finished product to verify it satisfies the documented requirements. Additional topics that span the entire product life cycle include interface management and control, risk management, tailing of process to meet organizational and project environments, configuration management, test strategies and trade-off studies.

Specific Goals and Objectives: Upon completion of this course, each student should be able to:
- Understand systems engineering as an interdisciplinary process and show its relationship to traditional engineering disciplines, applied science and program management.
- Demonstrate its value in the development of products, processes, and services.
- Explain fundamental concepts such as defining internal/external customer's needs early in the development cycle, generating requirements, selecting alternative solutions, testing and measuring of solution development relative to requirements.
- Access case studies, templates, and checklists that support the systems engineering approach.
- Tailor the general Systems Engineering Management Plan to the unique requirements of a specific organization and project.
- Utilize automated tools for report writing, tracking of requirements, capturing solution alternatives (e.g., trade studies), performance, cost and scheduling.
- Apply basic risk analysis and management techniques to product development.
- Form and maintain successful interdisciplinary and cross-functional teams.
- Apply standards (ISO, EIA, and IEEE), the SEI Capability Maturity Models - Integration (CMM - I) throughout the development process.

http://www.eas.pdx.edu/Systems/program/descriptions.html#SYSE%20591

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

6. Cornell University

Applied Systems Engineering I. Course topics:
1. Requirements analysis: Quality function deployment; Performance measures and design for X; Life cycle costing; Systems reliability
2. The Decision Making Process: Multi-attribute decision making; Team dynamics; Risk management
3. Systems Engineering Technical Process: Evaluate available information; Identify performance measures; Behavioral and functional analysis; Structural synthesis; Tradeoff analysis; Build and test plan
4. Systems Engineering Tools: Dynamic Systems Modeling and Simulation; Feedback control; Optimization
5. The build and test plan: Implementation issues; Prototyping and verification
6. A Unifying Systems Design Exercise

http://www.systemseng.cornell.edu/index.cfm?page=core

7. Johns Hopkins University

645.462 Introduction to Systems Engineering (graduate level – not undergraduate). This course covers the application of systems engineering principles and methods to the management of engineering efforts in technical development programs, as well as the variation in responsibilities and techniques as a project moves from initial mission statement through engineering design to deployment. Topics include requirements analysis, interface definition and control, system trade and sensitivity studies, concept definition and assessment, system design and integration, system test and evaluation, and software system fundamentals from a systems engineering perspective. Special topics include modeling and simulations, quality teams, and engineering processes, which are discussed from a system viewpoint. Students are introduced to a knowledge base for the functional allocation and analysis of complex systems. Students address typical systems engineering problems that highlight important issues and methods of technical problem resolution. *Prerequisites:* An engineering, science, or mathematics degree and two years experience in science or engineering.

http://ptesrv.apl.jhu.edu/03_04_catalog/sedesc.html#645.462

8. Massachusetts Institute of Technology

Computer System Engineering - Spring 2004
Prereq.: 6.004 (and, by implication, 6.001 and 6.002)
U (2), 5-0-7, CI-M. Topics on the engineering of computer software and hardware systems: techniques for controlling complexity; strong modularity using client-server design, virtual memory, and threads; networks; atomicity and coordination of parallel activities; recovery and reliability; **privacy, security, and encryption**; and impact of computer systems on society. Case studies of working systems and readings from the current literature provide comparisons and contrasts. Two design projects. Students engage in extensive written communication exercises. Enrollment may be limited. 4 Engineering Design Points.

http://web.mit.edu/6.033/www/general.html

9. University of Arizona

SIE 250 -- Introduction to Systems Engineering (3 units). *Description***:** System modeling; the elementary constructs and principles of system models including discrete-time, discrete-state system theory; finite state machines; modeling components, coupling, modes, and homomorphism. System design; requirements, life-cycle, performance measures and cost measures, tradeoffs, alternative design concepts, testing plan, and documentation Applications and case studies from engineering. http://catalog.arizona.edu/2003-04/courses/041/SIEx.html

10. University of Minnesota

Principles of Systems Engineering. *Description*: This course emphasizes a process which ensures that systems are designed, developed, and implemented in accordance with their intended usage through an integrated introduction to systems methodology, design, and management with a comprehensive overview of systems engineering as a professional and intellectual discipline, as well as its relation to other engineering disciplines.

Program Overview. Systems Engineering Principles examines the development of complex systems-of-systems by emphasizing the role of systems engineering and systems integration, processes, procedures, tools, and operating environments. Specific topics include operations analysis as necessary to understand the environment in which the system is to be used, synthesis of quality requirements, requirement analysis and issue resolution, requirements allocation to components, and requirements management. Other important topics covered include definition of systems boundaries, logical and physical architecture development, design reuse, decision-making, and technical reviews.

Upon successfully completing this program you will be able to:
- Understand basic concepts of systems engineering and the development of complex systems
- Understand integrated introduction to systems methodology, design, and management
- Understand a systems-design process
- Provide an overview of systems engineering as a professional and intellectual discipline, and its relation to other engineering disciplines

http://www.cce.umn.edu/events.nsf/Business/A3A44268A89C071386256E29007D7763

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Appendix B

It may now be time for those in the SE field to conduct research on how the information assurance models will fit into the SE models and objectives. This could assist in meeting the needs of practitioners and/or students learning to be practitioners. An avenue for this type of research is through the INCOSE SECOE.

The INCOSE System Engineering Centers of Excellence (SECOE) is a virtual collaboration of academic and industry researchers to advance the state of knowledge about systems engineering. SECOE participants are individuals with the desire to foster empirical and theoretical research into the engineering of complex systems. One of the core SECOE areas of research is SE Methods. According to SECOE the goal of the SE methods research topic is to develop a theoretical basis for known methods while extending the processes with new theories and new methods. Methods from other fields may also apply to advance systems engineering. Theoretic and practical constraints will bind each specific method to help practitioners know how and when to use it. Specifically, improvements in systems engineering methods are needed to (1) articulate and establish shared visions of problems, (2) identify and design alternative solutions, (3) perform trade studies and make decisions, (4) assess and manage risks, (5) verify and validate solutions, and (6) capture all information generated in the process. (INCOSE SECOE Research Agenda 2003.)

References

[1] International Council on System Engineering (INCOSE). http://www.secoe.org/intro.htm

[2] Massachusetts Institute of Technology, Systems Engineering Group. Website: http://web.mit.edu/6.033/www/general.html

[3] Portland State University, Systems Engineering, College of Engineering and Computer Science. Website: http://www.cecs.pdx.edu/Systems/program/

[4] Portland State University, Systems Engineering, College of Engineering and Computer Science. Website: http://www.cecs.pdx.edu/Systems/program/

[5] IEEE Std 1220-1998 (December 1998, copyrighted January 1999). IEEE Standard for Application and Management of the Systems Engineering Process. IEEE: New York, NY. (Revision of IEEE Std 1220-1994) (p. iii)

[6] [7] Information Assurance Technical Framework Forum (IATFF) (undated). "Introduction to the Information Assurance Technical Framework Forum. Available at the IATF website: http://www.iatf.net/file_serve.cfm?chapter=introduction.pdf

[8] Information Systems Security Handbook, Release 1.0, February 28, 1994. National Security Agency, Central Security Service. Only available for official USG use.

[9] Information Assurance Technical Framework (IATF), Version 3.1 (September 2002). National Security Agency, Information Assurance Solutions, Technical Directors; Fort Meade, MD.

[10] IATF, Chapter 3, p. 3-3 to 3-4

[11] INCOSE System Engineer Center of Excellence (SECOE) Research Agenda http://www.secoe.org/agenda.htm#20

Websites

http://wseweb.ew.usna.edu/wse/systems/Courses/es402.htm
http://www.gmu.edu/departments/seor/courses/syst-undergrad-courses.html
http://www.virginia.edu/registrar/records/ugradrec//chapter10/chapter10-3.htm
http://www.sie.arizona.edu/course_pages/
http://www.eas.pdx.edu/Systems/program/descriptions.html#SYSE%20591
http://www.eas.pdx.edu/Systems/syl/approach.html
http://www.cce.umn.edu/events.nsf/Business/A3A44268A89C071386256E29007D7763
http://catalog.arizona.edu/2003-04/courses/041/SIEx.html
http://web.mit.edu/6.033/www/general.html
http://ptesrv.apl.jhu.edu/03_04_catalog/sedesc.html#645.462
http://www.systemseng.cornell.edu/index.cfm?page=core