Homeland Security and the IE Curriculum

Marlin U. Thomas
School of Industrial Engineering, Purdue University

Abstract

The increased concern and awareness of threats to our homeland security resulting from the nine-one-one tragedy has changed our lives and altered our priorities in essentially all engineering decisions. While security is not a new design issue in engineering, this increase in social significance and public demand will naturally impact the practice and curriculum in industrial engineering. This paper reviews the areas of industrial engineering where homeland security is critical and provides some thoughts on integrating security and antiterrorism into the entry level professional IE curriculum.

1. Introduction

Homeland security has been a U.S. priority since the formation of our nation and throughout history our goal has been to provide citizens with a secure environment that is free of fears of any attacks or invasion of our homeland. This is largely the basis for maintaining a strong military force. In addition, we also have a network of federal, state, and local civil defense organizations that organize and direct preparedness and recovery plans for providing emergency relief to citizens during major disasters. Community alert programs such as air raid drills, training programs for schools, fall-out shelters, and emergency medical treatment plans are examples of our civil defense programs that support homeland defense. Prior to *Nine-One-One* we did have a sense of being a secure country and certainly without any thoughts of terrorist attacks on our cities. Unlike many other countries, threats of major catastrophes and disruptions in life style were of little to no concern in the U.S. The nine-one-one tragedy has changed this perception and altered priorities throughout our society. This has also made a tremendous impact in engineering and related professions, including the industrial engineering profession. While security is not a new design issue in engineering, the increased social significance of concerns of terrorism has elevated it to a much higher level. This will naturally impact the field of industrial engineering (IE).

IE is the most diverse of the engineering disciplines, emerging from mechanical engineering, management, psychology, and statistics. It evolved out of industry needs for efficient work systems and processes for better utilizing workers in factory operations in early 1900. The early focus was on time management and work simplification but soon included standards for conformance quality and extended beyond the factory floor. Some of the earliest research in IE was the study of bricklaying by Fred Gilbreth[1]. Today, IE is practiced throughout private and public sectors, including government and service industries. While many entry level professionals still enter the manufacturing sector, the largest number are found in the service industries such as airlines, hospitals, banks, and logistics organizations. In all cases they are engaged in the development and management of systems and processes that best utilize people, equipment and other resources that will provide products or services at an optimum level of performance. For a complete review of the evolution of the IE discipline from inception to modern day practice and applications see Emerson and Naehring[3], Martin-Vega[9], and Billings et. al.[2].

All engineering disciplines focus on public welfare and safety, and share the objective of pursuing optimal performance in the design, development and operations of systems. They also have important roles in national security and homeland defense. IE deals more with the human aspects of engineering systems and encompasses a broader overall system perspective than the other engineering disciplines, and therefore suitable for a more strategic and planning focus on homeland security measures for production and service systems. Industrial engineers are also equipped with analysis and quantitative skills for analyzing and evaluating security related decisions that involve risk and uncertainties. Consequently, IE is the obvious discipline to take lead in integrating methods and processes for implementing security measures in line with our homeland security policy[10].

In this paper we will review the areas of IE that directly relate and are critical to homeland security and provide some thoughts on integrating security and antiterrorism concepts into the entry level professional program. Our objective is to provide IE's with the proper tools for designing and developing systems that provide minimum risk from terrorism and maximize the safety and well being of the public. We start in Section 2 with a summary of the U.S. Homeland Security policy. The policy is quite extensive and covers six critical mission areas. Two of these areas: protection of critical infrastructure, and emergency preparedness and

response are directly relevant to IE. In Section 3, we examine these areas in detail. The role for IE is to provide methods and techniques to minimize the vulnerability of industrial systems to terrorism. IE's are educated in systems integration and quantitative methods though their major focus is generally to minimize costs and maximize quality in production and service systems. In Section 4, we examine the key core areas of the undergraduate curriculum for inclusion of security and antiterrorism concepts and issues and propose a framework for a dedicated course. Some concluding remarks are provided in Section 5.

2. U.S. Homeland Security

2.1 Strategic Objectives

The National Strategy for Homeland Security[10] provides overall guidance to federal, state, and local government; the private sector; and individual citizens on steps to improve the security of our homeland. The strategic objectives are to: prevent terrorist attacks within the United States, reduce our vulnerability to terrorist attacks, and minimize the damage and gain recovery for attacks that do occur. What is different about this strategy from ordinary defense is that the terrorist enemy studies our preparedness, and seeks out targets based on our weakness areas and then will pursue attacks with chemical, biological, radiological, and nuclear weapons to create major damage and destruction. So clearly, our initial thrust is to eliminate the possibility of attacks through significant efforts to prepare and achieve a level of readiness that would deter such attacks. State and local governments are responsible for funding, preparing, and operating emergency services that will respond to terrorist attacks. Private industries are to provide the information systems, detection equipment, vaccines and other technologies for coping with terrorism. The public is called upon to be proactive in promoting awareness and communications to achieve a national effort to detect, prevent, and, as necessary, respond to terrorist attacks.

2.2 Critical Mission Areas

The focus of the homeland security initiative is aligned into the following six critical functional areas; three that are aimed at preventing terrorist attacks, two at reducing our vulnerabilities; and one on minimizing damage and the recovery of attacks that do occur.

(1) Intelligence and Warning—intelligence and warning systems that provide early warning of attacks to allow for preemptive and protective action.

(2) Border and Transportation Security—integrated border and transportation security that provides reliable flow of people and logistics while preventing terrorist intervention.
(3) Domestic Counterterrorism—legal methods for identifying and dealing with terrorists and those who aide them.
(4) Protecting Critical Infrastructure and Key Assets—improve protection of elements that make up our physical and virtual networks that are critical to our infrastructure such as energy, transportation, and internet.
(5) Defending against Catastrophic Threats—provide unified effort for developing new approaches for detecting threats and protective methods for countering terrorism.
(6) Emergency Preparedness and Response—develop an integrated system that consolidates federal response plans with state and local governments and engages the American public for responding to threats and attacks in the U.S.

These areas focus on improving and integrating current defense programs and organizations into an effective national network system for detecting, preventing, and responding to acts of terrorism. All of these functions are important to industrial engineers and other disciplines as well, but areas (4) and (6) are most directly related to the conventional practice.

3. IE Relevant Mission Critical Areas

Industrial engineering deals with the design, development and implementation of people, machines and information resources for producing products and services. The types of product or service systems are based on their particular purpose and can vary significantly among numerous domains of application such as factories for producing metal fabricated parts and assemblies, airline industries, health care delivery, public utilities, parcel delivery services. The key elements of IE practice are people, processes, and products; and the focus is on achieving optimum performance and continuous improvement, often in allocating scarce resources. IE's were initially called efficiency experts during the early years of development of the profession and today they are sometimes characterized as productivity engineers, change agents, and system integrators. The common functional areas of industrial engineering are given in Table 1. Most industrial engineers are engaged in one or more of these areas and over the course of their career they will have rotated through all of them as an engineer, manager, or in the development of decision support systems that involve them. IE's are involved in strategic planning and management control decisions as well as operational decisions to assure the effectiveness in

carrying out specific tasks that relate to these functions in Table 1. For a detailed discussion of the functions and types of decisions that are directed by IE managers see Pritsker[11].

Table 1. Functional Areas of IE from Turner, Mize, and Case[14]

Production Engineering	Quality Control
Facilities Location	Financial Management
Facility Layout	& Engineering Economy
Work Measurement and Design	Personnel Management
Financial Compensation	Management Systems Design
Operations Planning and Control	Material Handling, Distribution & Routing

3.1 The Role of IE in Homeland Security

There are specialty areas embedded among those functions listed in Table 1 such as human factors and ergonomics, reliability, manufacturing, and information systems that are common areas of practice for many industrial engineers. IE is diverse, much more so than other engineering disciplines and it is practiced widely throughout private and public sectors of society. IE managers influence decisions at strategic, management control, and operational levels of organizations. The overall systems perspective and the experiences that industrial engineers develop through the key elements of operations and organizations prepares them well for upper management as a career option.

The basic strategy for homeland strategy is to detect, prevent, and respond to threats and acts of terrorism. So the first initiative is awareness to terrorism. Employees should understand the types of terrorist events that could occur and the appropriate emergency procedures that are to be followed given such occurrences. The general order of priorities is to first protect and ensure the safety and well-being of personnel; then protect the assets and property at risk; and thirdly, resume the operations.

3.2 Protection of Critical Infrastructure and Key Assets

Critical infrastructure and key assets are those systems and assets that are vital to our national needs and without them our safety, economic security, and health would be at high risk. The following sectors have been identified in National Security Strategy for Homeland Security[10] as being critical:

Agriculture	Information and Telecommunications
Food	Energy
Water	Transportation

Public Health	Banking and Finance
Emergency Service	Chemical Industry
Government	Postal and Shipping
Defense Industrial Base	

These industries, being crucial for our security and survival are likely targets for terrorism and must therefore receive top priority in protection. Strategies for protecting systems and assets in particular industries will depend on the types of attack such as chemical and biological weapons against our food and water resources, bombs and explosives against transportation and logistics flows, and cyber attacks on our information systems. To detect and prevent these attacks, antiterrorism methods need to be incorporated throughout the design and operations for these critical industries. The following IE areas are especially important in carrying out these measures:

Facilities location and layout design
Operations planning
Inventory planning and control
Material handling and distribution
Technical data and information systems
Transportation, packaging, and handling
Analysis of queues and bottlenecks

The basic facilities planning problem has five physical components: layout, materials handling, communications, utilities, and buildings[6]. Design alternatives are developed through consideration of input flows and internal transfer of materials, supply chains, information support such as digital circuitry, shielded cable, and security equipment; for outputs of products to warehouses, retail centers, or other transfer locations. The relationships among these components are analyzed relative to requirements of usage and efficiency gains in achieving the mission and purpose for the facility. Facilities planning and design decisions involve multiple criteria, but for most industry applications these decisions tend to be more cost based in the final evaluations. Under the homeland security strategy, facilities for our critical infrastructure and key assets will require more strenuous constraints on protection from terrorist attacks. System vulnerability and security measures become overriding factors in evaluating alternative designs for these systems.

Methods and procedures are available for assessing the risk and vulnerability for critical facilities. These methods are similar to work place design procedures, consisting of identifying

and classifying categories of risk according to hazard priority, structure integrity, operational vulnerability, and other information that relates to potential damage and threats. The U.S. Coast Guard administers a facility vulnerability and security measures self assessment Form CG-6025 under the Code of Federal Regulations for Facility Security.

3.3 Emergency Preparedness and Response

A second key critical mission area for homeland security that is particularly adaptable to industrial engineering is emergency preparedness and response to acts of terrorism. National strategy calls for readiness preparation that will result in minimum damage and facilitate effective recovery from future attacks. At the national level the process for disaster-response operations is outlined in the *1992 Federal Response Plan* prepared by FEMA in accordance with Public Laws 93-288/110-707, which provides architecture for a systematic and coordinated response plan for all government agencies. The more detailed plans that cover the specifics for transportation, health and medical services, public works, and other logistics support functions are delegated to state, regional and local governments. Under current homeland security policy the contingency planning for threats from terrorist activity is included in these planning and readiness functions. In addition, many companies and organizations have emergency teams that are deployed during crises for dealing with situations that are specific to their mission, vulnerability, and impact on public safety and security. Some examples are the chemical processing industries that produce toxic by-products, nuclear facilities where special expertise is required to respond to incidents, and public utilities. Since the nine-one-one attacks many other organizations have implemented emergency response plans as well. Under the national homeland security policy all response teams, including industry teams and civilian volunteers are coordinated to ensure overall effectiveness in providing the required rescue and recovery support for society.

3.3.1 Contingency Logistics Support Process

Terrorist attacks can require significant contingency operations for aiding victims and rectifying infrastructure. Contingency operations are largely logistics functions for procurement and acquisition, material handling and packaging, transportation, and distribution of supplies, materials and equipment required for the operations. These operations can vary immensely in magnitude, intensity, and duration but in all cases they extend over three distinct phases: mobilization and deployment, sustainment, and recovery operations[13].

Though contingencies occur at random there are generally plans that allow at least the initial guidelines for developing the logistics requirements and executing the actions required to support the mobilization and deployment. The relative resource profile for a contingency operation is shown by the ramp function in Figure 1. The deployment phase starts at a time t_0 marking the beginning of the contingency and extends throughout the mobilization and force build-up to a time t_1. On location an infrastructure is developed for the operation and interface with government and other participating organizations, and the service center support for food and supplies, medical, transportation, and so forth is implemented as required.

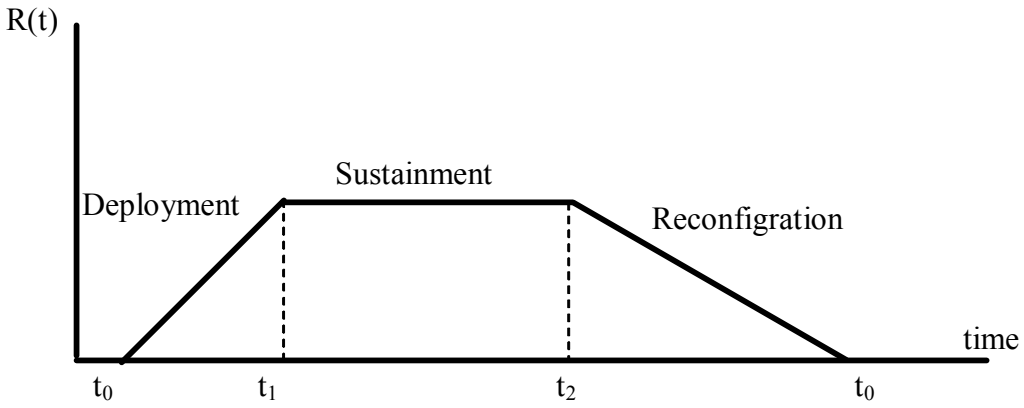

Figure 1. Lifecycle profile of a contingency logistics system.

At time t_1 the build-up is completed and the operations continue throughout what we call the sustainment phase. During this phase the nature of the operations and logistics requirements can change with the tempo and operational conditions but the basic processes and structure are all in place. The length of the sustainment period, depending upon the contingency could be weeks, months, or years.

At some point in time t_2, the operation is terminated by completion of the mission or by directive of higher authority. During this phase the infrastructure is transferred or modified for local conditions, service centers for supporting the mobilized personnel and equipment are phased down or collapsed as necessary to accommodate declining demands as redeployment occurs. Supplies and assets are re-distributed and the equipment and personnel are returned.

Contingencies by their very nature involve randomness and uncertainties. There are uncertainties with the initial occurrence, the type and magnitude of the operation, and the availability and readiness of the resources. The key to effective response-recovery operations is to maintain contingency plans that will maximize readiness to respond. Contingency planning is

an ongoing activity that requires skills in organizing and managing logistics, modeling and developing scenarios for plans, and analyzing risk and uncertain decision alternatives.

4. Proposed Curriculum Update

The elevated importance and need for public protection for security against terrorism adds new challenges for industrial engineering. Industrial engineering functions must include the latest methods and techniques for detection, prevention, and response strategies to counter acts of terrorism in the design, development and evaluation of systems. Consequently, it is imperative that the IE curriculum is updated to support this critical need. The objective is to ensure that systems design and development decision problems include security in parallel with the importance of cost, efficiency, and safety. So the question is how do we integrate homeland security into the IE curriculum?

The proposed plan for accomplishing this is to selectively infuse homeland security and related topics and applications into core courses where it makes sense, and implement a new course in security based IE design.

4.1 Security Skills for Practicing IE's

The basic undergraduate core industrial engineering program today ranges from 120 to 136 semester credit hours, of which 6 to 10 courses are in industrial engineering, 10 to 14 in engineering science, with the remaining from mathematical, natural and social sciences and liberal arts. The following nine courses are the core courses that are common to most programs in the U.S. (see Kuo[7]):

1. Capstone Design
2. Deterministic and Stochastic OR Models
3. Engineering Economy
4. Ergonomics and Workplace Design
5. Facilities Design
6. Inventory and Production Control
7. Production and Manufacturing Systems
8. Quality Control
9. Simulation

While the contents of these courses has changed over time, through research advances, new technology, and societal needs, the courses themselves have remained much the same over the past several decades. The current need for enhanced homeland security is indeed a societal need that calls for such updates and revisions to the basic curriculum.

All of these courses are candidates for adding homeland security topics through examples and applications of methods and concepts. However, the operations research (2) and simulation courses (9) are particularly suitable for implementing applications and examples dealing with detection and response to terrorist attacks. Facilities Design (5) and the capstone design course (1) are obvious courses that can readily be revised to include design issues. The following two examples are provided for illustration purposes.

4.1.1 Airport Security System

A schematic diagram of the flow of customers through an airport security system is shown in Figure 2. Customers arrive to their respective airline terminal and enter a queue to await their turn for an available agent or e-ticket machine for initial service for one or more of the following: check in for their flight, purchase a ticket, select seats, obtain a boarding pass, and check luggage. Upon completion of service at the airline counter customers proceed through security where they pass through an x-ray machine. Carry-on items and selected metal products are transferred into trays and passed through a conveyor as the individuals walk through an x-ray. Articles are then retrieved from the tray and they proceed on to the gate and await boarding instructions. Meanwhile, as customers are passing through security and waiting to board their flight, selected luggage is randomly chosen for inspection by security agents. The luggage is opened, visually inspected, and scanned for unauthorized articles. It is then repacked and labeled as having been inspected and passed on for transfer to the cargo section of the airplane. After the boarding announcement has been made and the process starts, selected customers are chosen at random for a final security check before boarding the aircraft. These individuals remove objects from their pockets and are again scanned by x-ray and then proceed to board the aircraft.

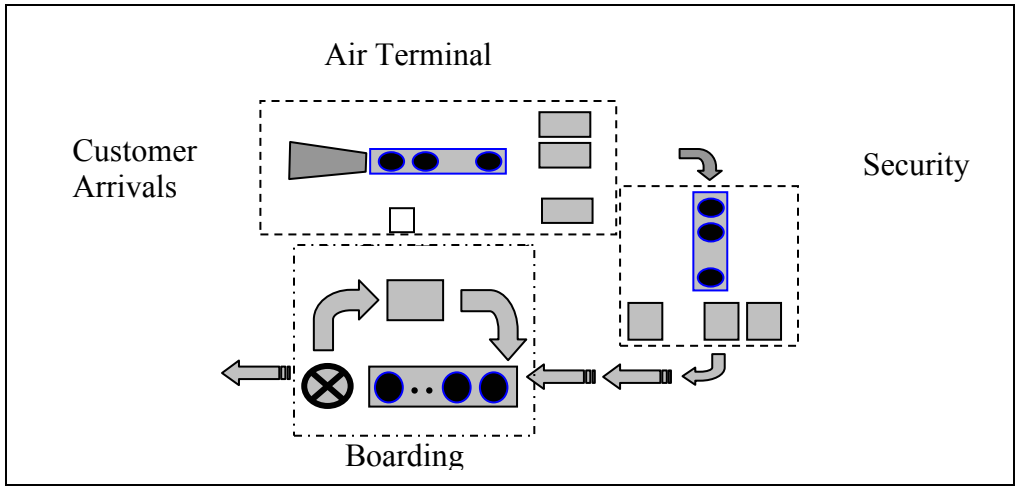

Figure 2. An airport security system for check-in and boarding flights.

Some important questions:

1. What is the likelihood of a terrorist act?
2. What antiterrorism processes can be built into the design?
3. How can the level of security be assessed?
4. How often should the system be inspected and updated to ensure reliability?

Concepts: cost/security tradeoffs, behavioral aspects of queues and security, conditions of steady-state versus transience, reliability, customer tolerance and vulnerability

Related IE Curriculum Topics: Descriptive modeling, queuing theory, simulation, decision analysis, reliability theory

4.1.2 Search and Detection for Recovery

A chemical processing plant has been bombed by terrorists leaving hundreds of people injured and trapped in the main facility. A crises action team is at the scene along with fire and rescue teams from the area. Gases are accumulating into the facility and the air ventilation system is down due to one of four control modules being damaged but the particular unit is not known. The modules are located at the north, south, east, and west extremes of the facility and all four must be working for the ventilation system to function. The emergency maintenance crew must locate and repair the module as soon as possible in order to restore air circulation to remove the assumed to be toxic gases from area while construction and rescue teams conduct recovery operations. Locating the source of failure is a serious problem due to the nature of the damage to the facility and the complexity of the modules.

Reconnaissance Information: Based on the information from the damage report by the crises action team, the probabilities of each of the four modules being the source of the failure of the ventilation system are estimated at $p_j, 0 \le p_j \le 1, i = N,S,E,W.$ Further estimates of times $t_N, t_S, t_E,$ and t_W required to test each module; and the probabilities $\alpha_N, \alpha_S, \alpha_E$, and α_W of the repair crew overlooking a failed module given that it is in fact the source of break down was made by the emergency maintenance crew.

Emergency Diagnostics Strategy: The objective is to find the failed module as soon as possible and the strategy will be to continue trouble shooting until it is found. Let $\delta = \langle \delta_1, \delta_2, ... \rangle$ represent the sequence for testing and note that a given module can be tested more than once since a failure can be overlooked by the maintenance crew. The optimum sequence for finding the failed module in minimum time can be determined by applying the following result from Thomas[12].

(1) Initially, determine δ_1 by selecting the largest from the ratios of p_i / t_i for i=A,B,C,D.

(2) If a module j is inspected and found not to be defective then the posterior probability of module i being the source of breakdown is given by

$$p_i' = \begin{cases} \dfrac{p_i}{p_j\alpha_j + 1 - p_j}, & i \neq j \\ \dfrac{p_i\alpha_i}{p_j\alpha_j + 1 - p_j}, & i = j \end{cases} \qquad (1)$$

(3) For each subsequent test k, select δ_k, k=2,3,…, that maximizes

$$\frac{p_i'(1-\alpha_i)}{t_i}, \quad i = A,B,C,D. \qquad (2)$$

Numerical Example: To illustrate the procedure suppose the probabilities of the crew overlooking the failed module are $\alpha_i = 0.10$ for all modules and the initial probabilities and troubleshooting times in hours are given as follows.

i	A	B	C	D
p_i	0.1	0.5	0.3	0.1
t_i	2	6	4	3

Start by computing the ratios:

$$\frac{p_A}{t_A}=.050,\quad \frac{p_B}{t_B}=.083,\quad \frac{p_C}{t_C}=.075,\quad \frac{p_D}{t_D}=.033$$

and selecting module B for the first to inspect and test. If this module is not found to be defective then the detection probabilities are updated, applying (1)

$$p_A{}'=\frac{p_A}{p_B\alpha_B+1-p_B}=\frac{.1}{.5(.1)+.5}=.182,$$

$$p_B{}'=\frac{p_B\alpha_B}{p_B\alpha_B+1-p_B}=\frac{.5(.1)}{.5(.1)+.5}=.091,$$

$$p_C{}'=\frac{p_C}{p_B\alpha_B+1-p_B}=\frac{.3}{.5(.1)+.5}=.545,$$

$$p_D{}'=\frac{p_D}{p_B\alpha_B+1-p_B}=\frac{.1}{.5(.1)+.5}=.182$$

To determine the second module to test, δ_2 we apply these posterior probabilities in (2) to obtain

$$\frac{p_A{}'(1-\alpha_A)}{t_A}=.082,\quad \frac{p_B{}'(1-\alpha_B)}{t_B}=.014,\quad \frac{p_C{}'(1-\alpha_C)}{t_C}=.123,\quad \frac{p_D{}'(1-\alpha_D)}{t_D}=.055$$

and thus select $\delta_2=C$. After testing C, if it is not found to be defective then the posterior probabilities computed at this stage become the prior probabilities, i.e. set $p_i=p_i'$, for i=A,B,C,D, and new posterior probabilities are updated using (1), from which it follows that $\delta=\langle B,C,A,D,D,...\rangle$ and the process is continued until the defective module is found.

Related IE Curriculum Topics: Search and detection, machine/maintenance diagnostics, stochastic OR models

Concepts: cost/security tradeoffs, vulnerability to terrorism, response-recovery

4.2 Security Based Design

Global competition and economic conditions compel most industries and organizations to aggressively follow a strategy to produce high quality products and services at minimum cost. The inherent need for enhanced homeland security now mandates security as an additional objective that must be included in planning and operations. Consequently, as discussed in Section 3 the role of IE has added responsibility for including security as a major criteria in decision making. The operational guidance for industrial engineering is to detect, prevent and

respond to threats and acts of terrorism throughout all functional areas. Industrial engineers understand risk and uncertainty but need to have a thorough understanding of (1) terrorism events and vulnerability, (2) contingency planning for terrorist events, (3) deployment options for responding to terrorism, and (4) vulnerability impact and antiterrorism procedures.

Implementation methods and techniques for the areas are yet to be developed for most applications. Some suggested objectives are as follows:

1. Establish standards of practice and methods for classifying facilities and processes with respect to the risk and vulnerability that exists in applications.
2. Develop operational readiness measures and alternative action plans for given breach levels of security.
3. Provide education and training for personnel on terrorism and security.
4. Integrate security into quality improvement strategies and plans that includes continuous improvements for security and antiterrorism.

4.2 A Notional Course Plan for Security Based Design for Industrial Engineering

Purpose: The purpose of the course is to prepare industrial engineering students with an understanding of terrorism and design concepts for implementing anti-terrorism and counter terrorism measures in systems design and development.

Objectives: The objectives for the course are to provide students with:

(1) knowledge of homeland security policy and strategy, including FEMA operations

(2) methods for assessing risk and vulnerability of facilities

(3) design concepts for antiterrorism

Level: senior

Prerequisites: probability, statistics, stochastic OR models, and facilities design

Topics:

1. Industrial Engineering Design
    a. Definitions and types of systems
    b. IE functions and design concepts
    c. Modeling
2. Terrorism and Homeland Security
    a. Types of terrorism and antiterrorism
    b. Homeland security policy

c. Critical mission areas for U.S. security
d. FEMA organization and role in homeland security

3. Detection Methods for Terrorist Threats
    a. Information and sensor technology
    b. Analysis methods for risk and uncertainty
    c. Pareto analysis and evaluation
    d. Network methods and critical resources
4. Prevention Methods
    a. Vulnerability assessment
    b. Reliability of security systems
    c. Design concepts
    d. Structuring critical event scenarios
5. Response and Recovery to Terrorism
    a. Contingency planning and operations
    b. Search and detection methods for maintenance recovery
    c. Emergency logistics
    d. Counter terrorism procedures

5. Concluding Remarks

There is no greater purpose in engineering than to provide people, our most important resource with a safe and secure living environment. Our national policy on homeland security is well defined and provides specific guidance on direction for critical areas that are vital to our national security, discussed in Section 2.2. Two of these areas; protecting critical infrastructure and key assets, and emergency preparedness and response have been identified in the paper as being most significant for industrial engineering practice. This in no way suggests that the others are of lesser importance. However, they tend to be more specialized areas that require a variety of technical methods and approaches for developing strategy and plans.

Homeland security is not new but since the *nine-one-one* events it has gained much greater concern to society and is now a national priority. All professional and technical communities are responding by seeking approaches and research programs to accelerate progress for homeland security. Operations research methods are particularly suitable for developing analysis and design methods for dealing with detection, prevention, and response actions for

terrorism. Operations research has a history of success in responding to needs for planning and allocating critical resources during emergencies (see Larson[8]). We now have need for revitalizing research in industrial engineering and operations research and related areas to provide new tools and skills for homeland security.

Homeland security should be integral to industrial engineering design. Industrial engineers need to be as security conscious as they are cost and quality conscious, and include security as part of continuous improvement strategies in cost and quality. The author recognizes that many IE educators are already actively engaged in updating courses and materials to address homeland security in the curriculum. This paper is an attempt to encourage and perhaps motivate others to get engaged and to stimulate further discussion on concepts and approaches to address this important revision to our program.

References

[1] ALDRICH, J.G., 1912. "The Present State of the Art of Industrial Management," Trans. of the ASME, Vol. 34, Paper 1378, pp. 1182-1187

[2] BILLINGS, C., J.J. Junguzza, D.F. Poirier, and S. Saeed, 2001. "The Role and Career of the Industrial Engineer in the Modern Organization," Ch. 1.2, "Maynard's Industrial Engineering Handbook, Ed. K.B. Zandin, Ch. 1.2, pp. 1.21-1.37

[3] EMERSON, H.P. and D.C.E. Naehring, 1988. , *Orgins of Industrial Engineering, the Early Years of a Profession*, Industrial Engineering and Management Press, Norcross, GA

[4] Executive Order Establishing Office of Homeland Security, October 8, 2001, The White House

[5] Executive Order on Critical Infrastructure Protection, October 16, 2001, The White House

[6] FILLMORE, W.E., 1992. Facilities Planning and Utilization, Sec. 13, *Maynard's Industrial Engineering Handbook*, Fourth Edition (Hodgson, W.K., Ed.), McGraw-Hill

[7] KUO, W., 2001, "Education Programs for the Industrial Engineer," Maynard's Industrial Engineering Handbook, Ed. K.B. Zandin, Ch. 1.3, pp. 1.39-1.53

[8] LARSON, R.C., 2004, "O.R. Models for Homeland Security," *OR/MS Today,* Vol. 31, No. 5, pp. 22-29

[9] MARTIN-VEGA, L.A., 2001. "The Purpose and Evolution of Industrial Engineering," Maynard's Industrial Engineering Handbook, Ed. K.B. Zandin, Ch. 1.1, pp. 1.3-1.20

[10] Office for Homeland Security, 2002, The National Strategy for Homeland Security, The White House, Washington, DC, July 16, 2002

[11] PRITSKER, A.A.B., 1990. *Papers·Experiences·Perspectives*, Systems Publishing Corp., West Lafayette, IN

[12] THOMAS, M.U., 1975. "On Minimizing the Mean Detection Time to Failures Subject to Detection Error," *Journal of Quality Technology*, Vol. 7, No. 2, pp. 59-66

[13] THOMAS, M.U., and M.A. Lawley, 2003. "Manufacturing for Contingency Logistics," Technical Memorandum, No. 2003-5, School of Industrial Engineering, Purdue University, 14p

[14] TURNER, W.C., J.H. Mize, and K.E. Case, 1978. *Introduction to Industrial and Systems Engineering*, Prentice-Hall, Englewood Cliffs, NJ

MARLIN U. THOMAS is Professor and past Head of the School of Industrial Engineering at Purdue University. He received his BSE at the University of Michigan-Dearborn, and MSE and PhD at the University of Michigan. He has held other academic appointments at Lehigh University, Cleveland State University, University of Missouri-Columbia, University of Wisconsin-Milwaukee, and the Naval Postgraduate School. He has also served as a Program Director for the National Science Foundation; Manager, Reliability and Warranty Analysis, Chrysler Corporation; and Development Engineer, Owens-Illinois, Inc. He is past National Secretary of ORSA, Chairman of the Council of Industrial Engineering Academic Department Heads, and IIE Past-President and member of the Board of Trustees. His research interests are in operations research with applications in reliability and contingency logistics. He has served on several editorial boards and is currently Associate Editor for *IIE Transactions* and is a Fellow of IIE, ASQ, and INFORMS. He is also a Captain, Civil Engineer Corps, U.S. Naval Reserve (Retired).