Homeland Security and Safety Engineering – Concept, Curriculum, and Challenges

Shekar Viswanathan and Howard E. Evans

School of Engineering and Technology
National University
11255 North Torrey Pines Road, La Jolla, California 92037, U.S.A.

Abstract

Events from 9/11 have highlighted the need for highly-educated technical professionals in the areas of security and safety. There has subsequently been a positive but limited response in terms of academic programs that emphasize ensuring the security and safety of people and physical assets. Such programs are relevant in the U.S. in part because the security problem here is a daunting task as we have a large influx of people and products into the country. Receiving far less publicity are the even greater unintended threats that can arise from natural disasters, human error, equipment malfunctions, and accidents incident to the manufacture, transportation, use, and disposal of potentially hazardous materials. Even though the United States is better equipped than most other countries to combat these problems, it still is vulnerable, as even its latest technologies cannot detect risks in all situations. It is with this in mind that a master's level academic program concentrating on Homeland Security and Safety Engineering has been developed.

The primary challenge of this program is to incorporate an array of courses in engineering and technology that are complementary, comprehensive, and relevant. A combination of experienced professionals from academics, public service, and private industries were brought together to develop a curriculum that identifies the common fundamentals and practices defining both the theory and effective practice of asset and people protection. Similar input was involved in making the determination to develop 'online' as well as 'in classroom' formats. This paper highlights the foundational concepts of this program, describes the involvement of multiple constituencies in its formulation, summarizes the curriculum developed, and provides an overview of challenges facing academicians in this field, including as a function of delivery method.

Background

History has recorded numerous terrorist activities against the U.S. and its interests both within and outside the country in the last 10 years alone. Each of these events provides unique perspectives on what should be done to protect assets and people. For example, On December 21, 1988, the unforgettable bombing of Pan Am Flight 103 in the sky over Lockerbie, Scotland, claimed the lives of 259 passengers and eleven victims on the ground. The investigation indicated that this incident was a result of a bomb planted in luggage by Libyan agents. Until 2001, airlines and regulators were struggling with how best to protect passengers from the threat of terrorist attempts to plant explosives due to lack of technology and processes.

A 1,200-pound car bomb exploded underneath the World Trade Center in New York on Friday, February 26, 1993, killing six people and injuring scores more. The entire bomb material was assembled at a cost of a few hundred dollars. The blast happened during the busiest hours at the World Trade Center. As a result, it caused panic in over 100,000 people who worked in or visited the 1,700-foot towers that day. Investigations into the attack revealed that the primary goal of the terrorists was to cause damage to assets and to kill people on a large scale.

On March 20, 1995, terrorists from the religious cult Aum Shinrikyo [1] released sarin, an organophosphate (OP) nerve gas, at several points in the Tokyo subway system, killing 11 and injuring more than 5,500 people. Sarin, was released in commuter trains on three different Tokyo subway lines and was concealed in lunch boxes and soft-drink containers placed on subway train floors. It was released as terrorists punctured the containers with umbrellas before leaving the trains. The incident was timed to coincide with rush hour, when trains were packed with commuters. This homemade nerve gas clearly showed the urban vulnerability to chemical attack by terrorists.

On the morning of April 19, 1995, Timothy McVeigh, an ex-soldier, parked a rented Ryder truck with explosives in front of the Alfred P. Murrah Federal Building, a United States Government complex, located in Oklahoma City. This resulted in a massive explosion that sheared the entire north side of the building, killing 168 people. Although the investigation indicated personal crusade as a reason for bombing the building, the incident clearly showed the extreme vulnerability of critical infrastructure protection of both public and private buildings within the U.S.

Overseas, more than 6,000 casualties have been caused by just three attacks: the bombings of military barracks in Saudi Arabia in 1996 and of U.S. embassies in Kenya and Tanzania in 1998. If three attacks with conventional explosives could injure or kill so many, the consequences of an attack using a nuclear, biological, or chemical weapon are much more immense. However, until September 11, 2001, not much effort was made to reevaluate our security and safety system.

Nineteen terrorists crashed two hijacked planes into the World Trade Center on the morning of September 11, 2001. The collapse of the twin 110-story towers resulted in 2,823 deaths [2]. These crashes were followed soon after by a commercial airliner exploding into part of the Pentagon. These events caused a loss of $ 11 trillion to the U.S. economy. Besides this, they caused $21 billion in property damage and insurance loss. A massive coordination effort by fire, safety, emergency response, security, and medical professionals was required to respond to this emergency. This tragedy clearly indicated that:

- Many corporations did not have a clear plan for people evacuation and disaster recovery.
- The government lacked initial centralized coordinated recovery capacity, and hence many were injured.

- The protection of public health was inadequate, and hence many people were exposed to debris and fire related emissions.

- The business continuity plan lacked many specifics including data recovery, communication, and safety enforcement.

- Structural steel of the twin 110-story towers of the World Trade Center was stripped of its fireproofing by debris from the aircraft impact and was weakened by the resulting fires, eventually causing the towers to collapse. Hence, reevaluation of fireproofing is essential.

- Communications networks that were thought to be redundant were actually running on the same infrastructure and constituted a crucial point of failure. However, other technologies including the Internet, geographic information systems, remote sensing, and mobile and wireless communications proved to be powerful tools for recovery.

Beginning in mid-September 2001, the United States experienced unprecedented biological attacks involving the intentional distribution of *Bacillus anthracis* spores through the postal system [3]. The full impact of this bioterrorist activity has not been assessed, but already the toll is large. A total of 22 persons have developed anthrax and 5 have died as a direct result [3]. More than 10,000 people were advised to take post-exposure prophylactic treatment because they were considered to be at known or potential risk for inhalational anthrax; thousands more became victims of hoaxes or false alarms, and several coworkers, friends, and family members of those directly affected developed severe anxiety attacks. The impact was not limited to the United States. Hoaxes involving threatening letters or powder-containing envelopes were reported from several countries; mail cross-contaminated with *B anthracis* was distributed to some U.S. embassies, and persons in remote corners of the world were advised to take prophylactic antimicrobial treatment.

Recent attacks on corporate and government computer networks have demonstrated the potential for damage if terrorists decide to perpetrate a cyber-attack. This is becoming more probable, as hackers and cyber-criminals more frequently target corporate and government IT assets [4]. Developing a vigorous plan for defending against such attacks must become more of a national priority. Most terrorist operations follow careful planning, including detailed casing and selection of targets. In this regard, perceived vulnerability, not just actual vulnerability, matters. Thus, security should be visible, but at the same time, it should not reveal particular measures taken. If this is compromised, the possibilities of being defeated by terrorists could increase significantly. Visible security may complicate some issues of corporate image and public relations, but its deterrent value regarding terrorists should be taken into consideration.

A terrorist attack is not required to wreak disaster. Hurricanes, earthquakes, tornadoes, floods, chemical plant explosions, and fires can be equally disruptive. The October 17, 1989, earthquake that rocked the San Francisco Bay area, the January 13, 1994, earthquake that shook Northridge, the four major 2004 hurricanes, namely Charley,

Frances, Ivan, and Jeanne that hit Florida and the Gulf coast, the December 3, 1984, Bhopal gas leak are vivid examples of catastrophes that have taught us many lessons. The 9/11 attack and the other previously mentioned events have highlighted the national (and to some extent international) need for highly educated and experienced professionals in the area of security and safety, and higher education bears a responsibility to respond to this need. To ensure a secure homeland, President Bush has created the Department of Homeland Security. Since then, there has been a positive but limited response in terms of academic programs focused on ensuring the security and safety of people and physical assets. The security problem in the U.S. is a daunting task primarily because we have a large influx of people and products into the country, and because we are exposed to a number of unintended threats arising from natural disasters, human error, equipment malfunctions, and accidents incident to the manufacture, transportation, use, and disposal of potentially hazardous materials. Even though we are more prepared than most other countries, we are still vulnerable because our latest technologies are not capable of detecting risks in all situations. It is with this in mind that a master's level academic program concentrating on Homeland Security and Safety Engineering has been developed.

Security and Safety Engineering, due to its special nature, represents an interdisciplinary area of study and application that brings together multiple fields of engineering, from the most traditional to the most technologically advanced and novel. Security and Safety engineering are very closely related disciplines. Although the development of an effective academic program in this combined field of Security and Safety may be complicated because of the wide range of knowledge that is necessary to span the profession, a well developed practical program can attract a wide audience nationwide. The challenge of this program is to incorporate a wide array of courses in engineering and technology. A well developed curriculum for this program would identify the common fundamentals and practices that define the theory and effective practice of asset and people protection and communicate these principles in an academic forum.

Description of National University and its Student Body

Founded in 1971, National University (NU) is an independent, nonprofit institution of higher education. Since its establishment, the university has dedicated itself to providing educational opportunities to a diverse population of working, adult learners. With more than 17,000 full-time students, National University is the second largest private, non-profit California institution of higher education, with a 32-year history of educating traditionally underserved populations. National University is ranked 7th nationally and 2nd in California for having awarded degrees to ethnic minority populations. Thirty-four percent of National's students are from minority populations and fifty-eight percent are female. NU is ranked sixteenth out of 3,000 in awarding graduate degrees to minority students. NU also received the California Council on Excellence (CCE) Eureka Award for Performance Excellence in 2002 and in 2003. National University's central purpose is to promote continuous learning by offering diverse instructional approaches, encouraging scholarship, engaging in collaborative community service, and empowering its constituents to become responsible citizens in an

interdependent, pluralistic, global community. National University students earn their degrees in a unique one-course-per-month format and attend classes at night so they can continue to move forward in the workplace. Their programs are accelerated so that they can complete their studies faster than at a traditional university. However, students can take only one course at a time. Each course has 40.5 hours of classroom contact, During this period, students are exposed to the challenges and intricacies of the subject taught in that class.

Although the introduction of the Homeland Security and Safety Engineering program is initially planned for a classroom environment offering, today's educators are asked to explore ways to expand options, particularly for those students who do not have the option of taking classes offered through traditional classrooms. Since additional higher educational opportunities can lead to challenging careers in today's competitive fields, it has been identified that an online program would be equally valuable to a traditional offering. It can conveniently accommodate many working adults.

Program Concept, Goals, and Outcomes

The overall goal is to develop a degree program in Homeland Security and Safety Engineering. Specific objectives for reaching this goal include the following:

- Design and offer a novel MS program that is suitable for working adults in a one-class-per-month format.
- Be accredited and approved by agencies/organizations such as ASSE, ASIS, ABET and WASC.
- Be flexible with a broad appeal to scientists, engineers, and technologists.
- Provide suitable knowledge and capabilities requisite to getting national certification from societies such as the Board of Certified Safety Engineers (BSP) and the American Society of Industrial Security (ASIS).

Upon completion of the MS program, graduates from Homeland Security and Safety Engineering will be able to:

1. Provide the security and safety demands required by the private and public sectors.
2. Understand and appreciate the complex technical and managerial issues related to security and safety.
3. Understand the engineering/technology behind security and safety solutions.
4. Apply quantitative and qualitative analytical skills and techniques to security and safety of assets.
5. Apply a multidisciplinary approach involving the integration of quality and risk analysis to the security and safety of assets.
6. Integrate state-of-the-art technological advances to the practice of modern security and safety engineering programs, including the use of information technology and supporting software applications.
7. Apply a global mindset to security and safety issues related to assets.

8. Assess the impact of security and safety issues for the operation of corporations and businesses and develop appropriate action plans through detailed engineering analyses and design.
9. Integrate tools and techniques, resources, organizational systems, and decision making processes for the successful implementation of security and safety plans.
10. Possess the knowledge necessary to become certified as a safety (CSP) and security professional (CPP).

Program Design, Curriculum Development, and Challenges

A primary challenge is to bring together in a cogent structure the wide array of technical courses relevant to security and safety needs. This can be approached by identifying the common fundamentals and practices that define the theory and effective practice of asset and people protection. Activities planned to meet the program goals and outcomes include the following:

1. Design a curriculum that effectively meets the needs of homeland security and safety;
2. Identify learning outcomes for each of the courses designed and select appropriate teaching materials such as textbooks, journals, and other online tools;
3. Develop teaching tools such as weekly lecture notes, tutorials, case studies, simulation and quiz materials to reinforce the learning outcomes;
4. Establish means of assessment for each course designed;
5. Select appropriate case studies and other tools that may be helpful in reinforcing the proposed program;
6. Collaborate with NU's online course design and dissemination staff to ensure effective incorporation of captioning, media-streaming, interpreting, and/or other accessibility features;
7. Collaborate with relevant faculty to ensure content integrity of courses adapted for online presentation;
8. Explore new educational technologies to enhance accessibility and appropriateness of instructional materials and media;
9. Consult with the public and security agencies experienced in the area of homeland security and safety;
10. Establish an assistive technology training center within National University's extensive library/Cybrary required by online students;
11. Support data collection and documentation of project activities and results to promote students' ease of access to the program and increased learning;
12. Ensure widespread dissemination of project activities and evaluation via national professional conferences, journal articles, and media coverage.

Figure 1 provides an overview of National University's Homeland Security and Safety Engineering programs. Table 1 provides a description of each course, and its learning outcomes.

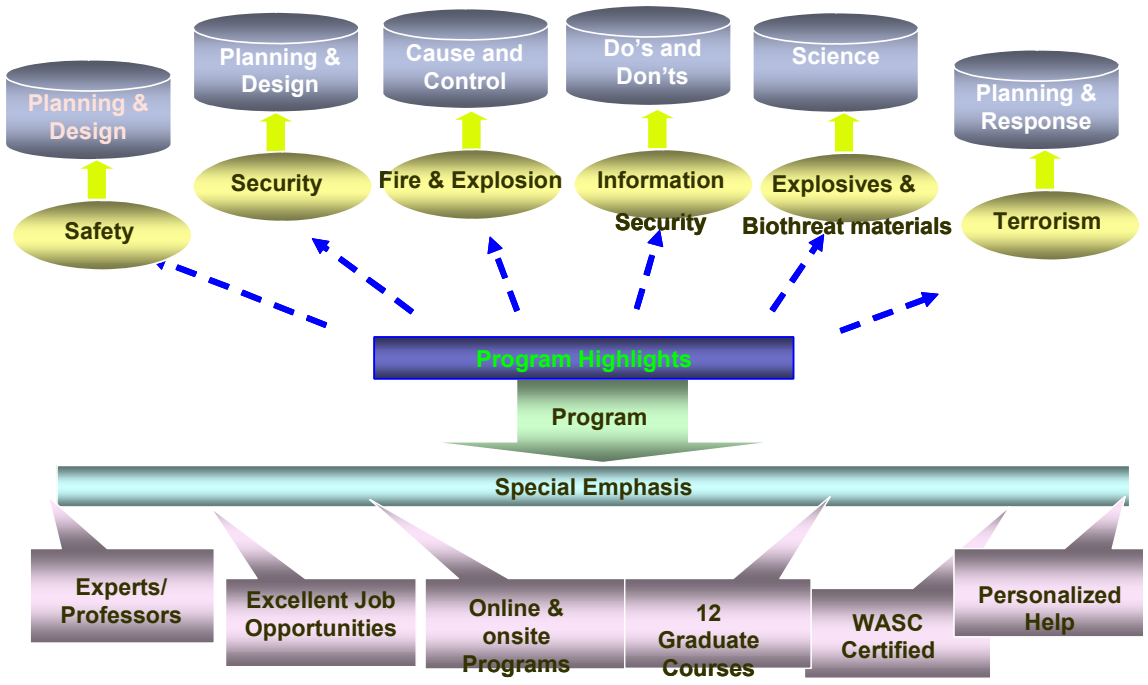

Figure 1: National University's Homeland Security and Safety Program at a Glance

A key precept that guided this program development is that this program must accommodate individuals with different learning styles, needs, and interests. A panel of experts from industries, law enforcement, military, and consultants were brought together to provide a detailed assessment of what courses should be incorporated in this program. In addition, informal consultations with other academic institutions offering similar programs were held to incorporate their experiences. To cater to this diverse population, each course is designed to accommodate a wide variety of teaching approaches and features. Specific features are incorporated so as to make the online and on-ground programs very effective. Some of them include video and audio presentations, special guest lectures by experts, case study analysis related to several real life examples, and field visits. Each course has been designed to incorporate background review materials relevant to a given course, test materials on various concepts, and continuous progress monitoring. Throughout the design and implementation of this program, consultations were sought from security and industry personnel, and from other relevant public sector agencies, in order to ensure that the program is relevant and effective.

One of the primary concepts of online education is the opportunity to offer students the possibility of "learning anytime, anywhere." For the purpose of this project, that is construed to mean that, to the maximum extent possible, all accessibility features must be designed to afford students access to education resources anytime, anywhere without the need for outside assistance. Whenever possible, accessibility is provided with built-in and/or interface design/content layout, utilizing appropriate, state-of-the-art assistive technology.

To receive a Master of Science in Homeland Security and Safety Engineering, students must complete 54 quarter units involving twelve courses, each course being worth 4.5 quarter units. Candidates for the program must possess a Bachelor's degree in engineering, engineering technology, or physical sciences or a closely related area from an accredited university. Interested students from other disciplines may be admitted to the program but may be required to complete additional courses. Non-degree students are not allowed to enter this program. For those who have a general non-science and non-engineering degree, admission is based on relevant experience and a set of program prerequisites.

Table 1: Description of Courses and Learning Outcomes

Course Title	Course Description	Learning Outcomes
Statistics for Safety and Security Professionals	This course provides practical grasp of the research designs and related statistical techniques needed to successfully tackle day-to-day problems in the safety and security area.	• Design Safety and Security research projects and programs. • Design and implement data collection and analysis procedures for safety and security related work. • Develop administrative control processes using data analysis and correlations.
Introduction to Safety Engineering	This course introduces the principles of general safety, and safety education. This course offers extensive coverage of all aspects of safety: home, fire, personal, recreational, occupational, and school. In addition, this course discusses methods of injury evaluation and easy-to-find and well-illustrated guidelines to avoid unsafe practices.	• Describe what safety is and how to assess it through statistical approaches. • Illustrate skills required to assess home hafety, fire safety, occupational safety, natural and man-made disasters, recreational safety and school safety. • Develop procedures/systems to minimize / eliminate safety related disasters.
Design and Evaluation of a Modern Safety Program	This course provides comprehensive coverage of occupational safety and health fields including concepts such as: technological changes that have introduced new hazards in the workplace; proliferation of health and safety legislation and corresponding regulations; health care and workers' compensation costs; and increasing incidents of workplace violence. This course introduces engineering concepts through case study analysis and provides	• Develop an easy safety checklist for doing safety audits. • Train people in health and safety issues they will face on the job, and prepare them for prevention or correction. • Develop reporting forms, enhanced enforcement policy; machine guarding and control of potentially hazardous mechanical and energy systems; fire

	hands on experience in developing a modern safety program.	standards; and hazard communication standards. • Conduct accident investigations on the types and causes of accidents and develop policies /procedures to eliminate/avoid them.
Introduction to Security Engineering	This course introduces security and loss prevention as well as an overview of the security field including risk assessment, physical security, personnel security and information security areas. It provides students with a solid introduction to security principles and focuses on security concepts and management in a post-9/11 world, including expanded coverage of terrorism and homeland security. It introduces students to the new threats and prevention strategies to more than 20 specific security applications in real world examples.	• Describe the roles of the security manger, and regulations of the security industry. • Identify and assess threats to security from natural, man-made and environmental disasters, and civil disorders and crimes. • Perform risk assessment, security surveys and develop contingency planning. • Develop levels of protection such as perimeter controls, surveillance systems, alarm systems, fire protection and human protection systems and advanced sensors.
Security Engineering - Planning and Design	This course provides comprehensive coverage of security planning in both new and existing facilities. This course covers real-world concepts on security design concepts, security evaluation and planning, building hardening, security technology, biochemical and radiological protection, security and emergency operations, and putting security into practice.	• Develop a comprehensive building security system and evaluation procedures. • Train people in security issues they will face on the job and prepare them for prevention or correction. • Evaluate security technologies and procedures for emergency and routine operations. • Conduct security investigations on the types and causes of security breaches and develop policies /procedures to eliminate/avoid them.
Chemical Process Safety Engineering	This course covers chemical process safety and provides an overview of safety evaluation of chemical plants. Emphasis on fundamentals is intended to help both the student and the practicing scientist to understand applicable safety concepts and to apply them in an appropriate manner. Details are examined for concepts such as process hazards checklists; hazards surveys; hazards and operability studies; and risk assessment techniques using probability theory, event trees, and fault trees.	• Describe what chemical safety is and how to assess it. • Conduct accidental / man made release of chemicals into atmosphere. • Perform hazards identification through hazards and operability Studies. • Conduct risk assessment through probability theory, event trees and fault trees. • Perform accident investigations and develop risk mitigation strategies.
Managing Information Security	This course introduces the computer security issue for every type of system, from traditional centralized systems to distributed networks and the Internet. Students will be familiarized with the state-of-the-art in networking; cryptography; program and operating system security; administration; legal, privacy, ethical issues, and much more.	• Describe what computer security issues are and how to assess them. • Demonstrate skills required to assess state-of-the-art in networking; cryptography; program and operating system security; administration; legal, privacy, and ethical issues. • Assess the security vulnerabilities and threats, and follows countermeasures

		to address them.
Fire and Explosion Engineering	Introduction to fire science; fire prevention, containment and extinguishment; methods of assessment of fire risks; hydrocarbon fires and explosions; methods of estimating explosion overpressures; dynamic response of structures to sudden overpressures; explosion detection, control and mitigation techniques; active and passive fire protection systems; escape routes; legal requirements.	• Interpret code requirements for fire safety. • Understand the concepts of fire severity and fire resistance. • Understand the behavior of structural elements and buildings exposed to fires. • Assess the fire performance of existing structures. • Develop control and mitigation techniques for fire prevention.
Science of Explosives and Biological Threat Materials	This course introduces forensic identification and detection of explosives including: basic classification; tagging of explosives; the detection of hidden explosives in airfreight, luggage, vehicles, and on suspects; etc. The course also covers biological threat materials and their assessment and control.	• Understand the science of explosives and biological threat materials and how to detect them using various concepts and methods. • Develop control and mitigation techniques for protection against explosives and biological threat materials.
Planning and Response for Terrorism	This course introduces the comprehensive and integrated principles behind chemical, biological, radiological, and cyber-terrorism. Also, designing and implementation of Incident Management System with appropriate response procedures for each of these terrorism and tactical violence incidents.	• Develop Incident Management System • Design and implement response procedures for terrorism and tactical violence incidents. • Develop procedures/systems to minimize / eliminate effects due to chemical/biological/radiological/explosive/ cyber-terrorism
Security and Safety Engineering Capstone Courses	These project courses focus on the application of safety and security engineering methods and processes learned through this program. The students are to select research topics under the guidance of instructor and conduct research and write a detailed report. Working in teams or as individuals under the guidance of their assigned faculty advisor, students clarify research topics and identify sources from which data is gathered in preparation for the project. Students then gather data and present their research in both written and oral form to the client organization, if applicable, and to other students and faculty.	• Evaluate and design critical safety and security systems for buildings and/or processes. • Write a Master's level research project/thesis based on the findings. • Define a research problem and/or an industrial / commercial case study. • Perform a literature review and methods used in the project. • Identify sources of data for the analysis and gather and analyze relevant data. • Identify, describe and use appropriate quantitative and analytical models for drawing conclusions. • Defend the project findings during oral presentation to faculty, class and, if applicable, to clients.

Program Evaluation

Each course has a clearly defined set of assessment requirements as shown in Table 2. Although a given instructor can change the type of assessment processes (number of assignments, number of questions, etc), everyone has to meet the minimum

rigor established in Table 2. Each instructor is evaluated by peers for teaching style and rigor applied. The lead faculty ensures that all requirements as set aside for the program are maintained. In addition to these evaluation measures, a qualified outside evaluator will be hired to measure program success, utilizing short-term domains related to ease of student access to this non-traditional program. Evaluation will incorporate formative evaluation measures, to provide techniques for improving the program as it progresses, as well as summative evaluation measures, to assess the achievement of program goals and objectives. Data obtained should be useful to other colleges and universities similarly interested in developing such a program.

Outcomes for this program will be measured by: 1) numbers of target student inquiries; 2) numbers of students contacted or enrolled; 3) comparisons of previous and current student education experiences; 4) student, faculty, and mentor assessments; and 5) faculty enhancement data, especially quantity and quality of teacher training

Table 2: Course Assessment Measures

Course Title		**Means of Assessment**							
		Mid-term Exams	Final Exam	Writing Assign-ments	Re-search Paper	Oral Presen-tation	Graded Home-work	Graded Partici-pation	Case Analysis
1.	Statistics for Safety and Security Professionals	X	X				X		
2.	Introduction to Safety Engineering	X	X	X			X	X	X
3.	Design and Evaluation of a Modern Safety Program	X	X	X		X		X	
4.	Introduction to Security Engineering	X	X	X			X	X	X
5.	Security Engineering - Planning and Design	X	X	X		X		X	
6.	Chemical Process Safety Engineering	X	X	X		X	X	X	X
7.	Managing Information Security	X	X	X		X	X	X	X
8.	Fire and Explosion Engineering	X	X	X		X	X	X	X
9.	Science of Explosives and biological threat materials	X	X	X		X	X	X	
10.	Planning and Response for Terrorism		X	X		X	X	X	X
11.	Safety and Security Engineering Capstone Course			X	X	X			
12.	Safety and Security Engineering Capstone Course			X	X	X			

opportunities. Long-term success of this program will be measured by increased numbers of individuals who successfully graduate and enter security and safety careers as a result of this unique educational opportunity.

References

1. Morita H, Yanagisawa N, Nakajima T, “Sarin Poisoning in Matsumoto”, Japan. Lancet 1995; 346:290-293.

2. Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, October 2004, ISBN- 0-16-072304-3.
3. Gerberding, J.L., Hughes, J.M, Koplan, J.P., "Bioterrorism Preparedness and Response"**,** *JAMA*. 2002; 287:898-900.
4. The White House Report, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", February (2003).