AC 2007-2836: A MULTIDISCIPLINARY MASTER'S PROGRAM IN HOMELAND SECURITY AND SAFETY ENGINEERING

Howard Evans, National University

Dr. Howard Evans was appointed founding Dean of the School of Engineering and Technology, National University, in October, 2003. He received B.S. degrees in Physics and Chemical Engineering from Brigham Young University, and a Ph.D. in Chemical Engineering Science from the California Institute of Technology.

Dr. Evans has over 20 years of executive and senior technical management experience at 3M Company and IBM Corporation, primarily leading multidisciplinary, global technical organizations responsible for R&D; new business and market development; manufacturing engineering; quality; environmental, health and safety; and others.

Before joining National University, he acquired 12+ years of voluntary involvement with higher education, including adjunct teaching and research in engineering at the University of Colorado and formal advisory involvement in both science and engineering at the University of Texas. Other past professional and academic activities include being a founding member and officer in the Central Texas Electronics Association; past chairman of IBM's Materials Shared University Research Committee; Ph.D. Recruiting Coordinator for IBM's Systems Technology Division; and executive sponsor for 3M division's student programs. He has published and presented widely in areas of surface science, electronic materials and processes, project management, and industry/university relations. He holds 4 patents and has received awards for excellence in technical innovation (IBM), technical authorship (IBM), teaching (University of Colorado), and scholarship (National Science Foundation).

Shekar Viswanathan, National University

Dr. Viswanathan is a Professor and Chair of the Department of Applied Engineering and Lead Faculty for Engineering Management and Homeland Security and Safety Engineering. He is the Lead for six full time and fifty two adjunct faculty members. His department offers three undergraduate and six graduate programs and has a student population of three hundred students. Dr. Viswanathan is an educator, researcher and administrator with more than twenty-five years of industrial and academic experience encompassing engineering and environmental consulting, research and development, and technology development. His career experience includes teaching at the University level, conducting fundamental research, and developing continuing educational courses.

© American Society for Engineering Education, 2007

A Multidisciplinary Master's Program in Homeland Security and Safety Engineering

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 number of 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 both within and outside the U.S. 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 [1]. 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 [2]. 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 1,700ft 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 [3] released sarin, an organophosphate (OP) nerve gas, at several points in the Tokyo subway system, killing 11 and injuring more than 5,500 people. The nerve gas, sarin, was released in commuter trains on three different Tokyo subway lines. Sarin was concealed in lunch boxes and soft-drink containers and 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 by the terrorists clearly showed the urban vulnerability to chemical attack.

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 [4]. 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 twin 110-story towers resulted in 2,823 deaths [5]. 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, it caused $21 billion property damage and insurance loss. 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.
- Business continuity plans 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 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 [6]. 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 [6]. 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 US 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 [7]. 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.

It does not require a terrorist attack 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 [8]; 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; San Diego Wild Fire, 2003 [9] are vivid examples of catastrophes that have taught us many lessons. The 9/11 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 George W. 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, science and management, 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 has been to incorporate a wide array of material from disciplines in: chemistry, biology, and physics; chemical, mechanical and civil engineering; operations planning and management; information technology and communications technologies; and others. 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 22,000 full-time students, National University is the second largest private, non-profit California institution of higher education, with a 36-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. Nationally, 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. These aspects of the NU mission align nicely with objectives of a program in security and safety engineering. In addition, 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. However, students can take only one course at a time. Each course has 40.5 hours of class room 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 was initially planned solely 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 as valuable as a traditional classroom offering. This

approach can conveniently accommodate many potential students regardless of geographic locations.

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-course-per-month format
- 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 Board of Certified Safety Engineers (BSP) and American Society of Industrial Security (ASIS).
- Incorporate Federal Emergency Management Authority (FEMA) Certifications (specifically ICS 100, 200, 700, 800).

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 for the protection of people and assets.
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 people and assets.
5. Apply a multidisciplinary approach involving the integration of quality and risk analysis to the security and safety of people and 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 people and 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.

Possess the knowledge necessary to become certified as a safety (CSP) and security professional (CPP) and pass FEMA Certifications (specifically ICS 100, 200, 700, 800)

Program Design, Curriculum Development and Challenges

A primary challenge is to bring together in a cogent structure the wide array of technical concepts 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 – regardless of discipline – then grouping these concepts together as they are linked in applications. These have then been divided into individual courses that are topic and application-specific, rather than separated into courses that are discipline-specific. For example, a course has been developed around the topic and application: *Design and Evaluation of a Modern Safety Plan*. This course synthesizes material from a number of disciplines all related to this specific application, including: chemistry and physics (science of safety and health hazards); laws and contracts (safety and health regulations); ethics and public relations (corporate responsibility); business (cost/benefit analyses, risk assessment, and profitability) and management (project management). Similar groupings have been done for each (topic and application-specific) course.

Activities planned to meet the program goals and outcomes included 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 text books, 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 public and private security agencies experienced in the area of homeland security and safety;
10. Establish an assistive technology training and reference center within National University's extensive library/Cybrary required by online students;
11. Ensure widespread dissemination of project activities and evaluation via national professional conferences, journal articles, and media coverage.

Figure 1 provides an overview of the underlying conceptual structure defined to guide overall development of National University's Homeland Security and Safety Engineering program. It is meant to represent the three key foundational characteristics of the program content as it supports the protection of people and physical assets: 1) integrated content (safety and security, prevention and response, accidents and terrorism); 2) interdisciplinary content; and 3) relevant content.

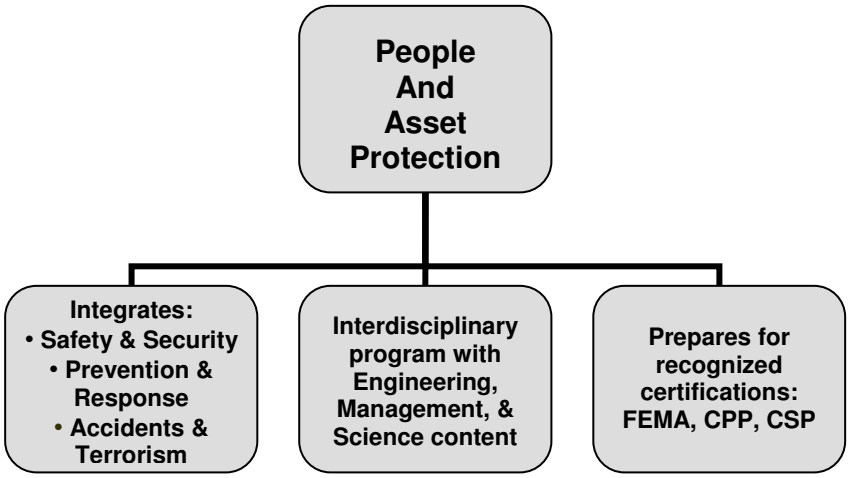

Figure 1: Foundational elements of National University's Homeland Security and Safety Engineering Program

A panel of experts from industry, law enforcement, military and consultants were brought together to provide detailed definition of what content – and, subsequently, what courses - should be incorporated in the program. Informal consultations with other academic institutions offering similar programs were held to incorporate their experiences. Figure 2 relates the primary topic and application areas around which courses are designed, and shows the basic skills and capabilities to be acquired for each area. Additionally, the figure ties in other key features: program length, accreditation, delivery modes, and faculty qualification. Table 1 shows the resultant courses with their associated, integrated, interdisciplinary and relevant content. It also lists the desired learning outcomes for each course.

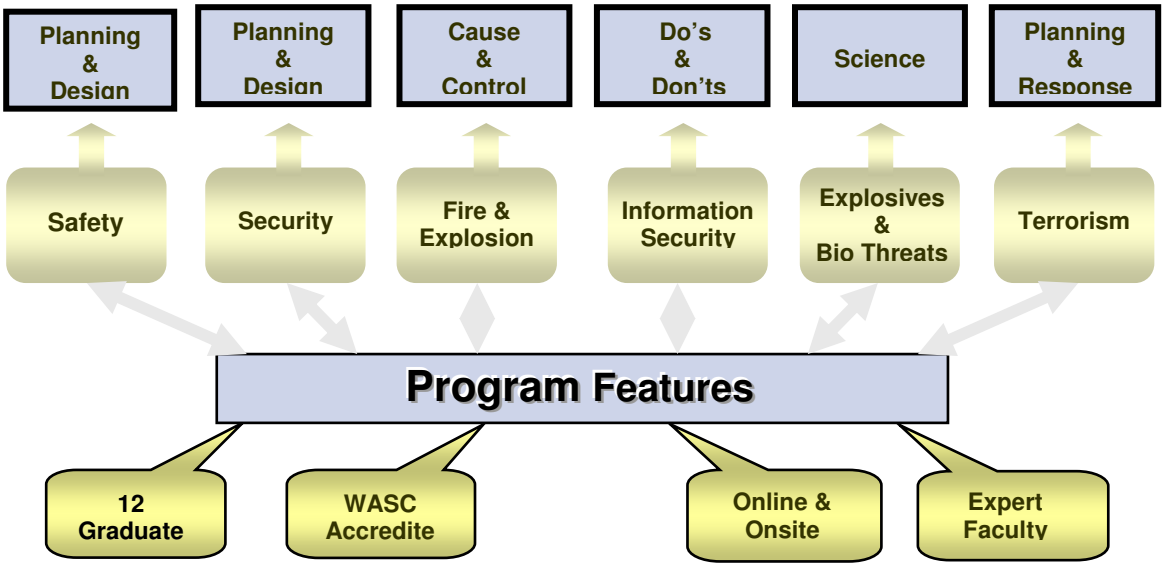

Figure 2: National University's Homeland Security and Safety Program at a Glance

A key precept that guided program development was the desire to accommodate individuals with different learning styles, needs, and backgrounds. 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 these include video and audio presentations, special guest lectures by experts, case study analysis related to multiple 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 continued with 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 with the need for minimal 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 will optimally 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 also be admitted to the program but may be required to complete additional courses. (Non-degree students are not allowed to enter the 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 including courses in chemistry, environmental science/engineering, and probability and statistics. Our original anticipation was that graduates with Bachelor's degrees in such fields as management, public administration, criminal justice and perhaps even information systems and information technology would find the program attractive, although this has not been borne out by the entering students thus far. To date, twenty-two students have entered the program. These students' undergraduate degrees include chemistry, electrical engineering, environmental engineering, industrial engineering, civil engineering, electronics engineering technology, and physics. Also, a significant number of students entering to date have Department of Defense background.

Table 1: Description of Courses and Learning Outcomes

Course Title	Course Description	Learning Outcomes
Emergency Management	The course details the Federal Emergency Management Agency (FEMA) (U.S), the Federal Response Plan (FRP), and the roles, responsibilities, and	• Understand the concepts of emergency management • Perform natural and technological hazard and risk assessment • Assess technologies and manpower

	interrelationship between FEMA and state and local emergency management systems. It also covers the changes in emergency management since the events of September 11, 2001, including mitigation, response, recovery, preparedness and communications.	needed for emergency management • Develop mitigation, response and communication techniques for emergency response
Disaster Management and Preparedness	This course offers training on disaster response and management in the face of natural and manmade catastrophes. The course provides training on methodological approaches to be adopted during a disaster. Specific topics include identifying the risks; preplanning for a disaster; eliminating, minimizing, and shifting risks; effective communications; and training for success	• Understand the concepts and response required during a disaster. • Understand the response required for a typical manmade or natural disaster • Develop an incident control system for response • Manage and coordinate response during a disaster
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 hands on experience in developing a modern safety program.	• 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 Standards; and Hazard Communication Standards. • Conduct accident investigations on the types and causes of accidents and develop policies /procedures to eliminate/avoid them.
Security Engineering - Planning and Design	This course provides a comprehensive coverage of security planning in both new and existing facilities. This course covers real-world concepts on security design, security evaluation and planning, building hardening, security technology, biochemical and radiological protection, security and	• Develop a comprehensive building security system and evaluation procedure. • 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.

	emergency operations and putting security into practice.	• 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, and 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 security vulnerabilities and threats, and follow 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	This course introduces forensic identification and detection of explosives including: basic classification; tagging of	• Understand the science of explosives and biological threat materials and how to detect them using various concepts and methods.

threat materials	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.	• 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 Systems 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. • 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. • Write a Masters level research project/thesis based on the findings. • Defend the project findings during oral presentation to faculty, class and, if applicable, to clients.

This set of course descriptions designates content from multiple disciplines, such as: chemistry, physics, applied physics, information assurance, laws and contracts, management, computer networks, sensor networks, environmental science and engineering, civil engineering, chemical and mechanical engineering, fire science, and information technology. Some of the engineering capabilities described by the learning outcomes include safety and security-related aspects of: problem identification and analysis; environmental assessment and control; design and analysis of processes, systems and networks; industrial design and evaluation; combustion science, and control and containment; risk analysis and assessment; structural dynamic responses; information technology; detection and sensor networks; technical project management; technical writing; verbal communication and presentation skills; teamwork; and others.

Program Faculty

The interdisciplinary, relevant and specialized nature of the program content requires a faculty with similar breadth, experience, and expertise. This has been achieved by combining a core of full time faculty with a talented adjunct faculty comprised of practicing professionals. Examples of faculty credentials include:

- Ph.D. in Chemical Engineering, P.E. License, > 20 years of private sector experience
- Vice President, consulting organization, CIH and CSP certifications
- Security Director for Jack in the Box, Inc., CPP certification
- Deputy Chief Operating Officer for Public Safety and Director of Homeland Security, City of San Diego
- Ph.D. in Engineering Physics with IT security background
- Safety Director for Olivenhain Municipal Water District, CSP certification
- Environmental Manager of ISP Alginates, P.E. License
- Cmdr, EOD Group 1, Explosive Ordinance Disposal, US Navy

The above mentioned faculty collectively have over 160 years of public and private sector experience.

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 for the program are maintained. In addition to these evaluation measures, an advisory group of external experts will be convened at regular intervals to assess program status, evaluate up-to-date relevancy, and advise on possible curriculum improvements and updates. 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 may be useful to other colleges and universities similarly interested in developing such a program.

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.	Emergency Management	X	X	X	X	X	X		
2.	Disaster Management and Preparedness	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			

Outcomes for the overall program will be measured by: 1) trends in the numbers of students enrolling; 2) student, alumni and employer surveys; and, 3) assessment of final student thesis and project reports and presentations by internal (faculty) and external expert review boards. Long-term success of this program will be reflected by increased numbers of individuals who successfully graduate and enter security and safety careers as a result of this unique educational opportunity.

References:

1. Dornstein, K, "The Boy Who Fell Out of the Sky" Random House, 2006; ISBN: 9780375503597.

2. U.S. Fire Administration / Technical Report Analysis, "The World Trade Center Bombing: Report Analysis", New York City, New York, USFA- TR-076, February, 1993.

3. Yanagisawa, M.H., N, Nakajima T, "Sarin poisoning in Matsumoto", Japan. Lancet 1995; 346:290-293.

4. U.S. Department of Justice Report, "Responding to Terrorism Victims: Okalahoma City and Beyond", October 2000.

5. Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, October 2004, ISBN- 0-16-072304-3.

6. Gerberding, J.L., Hughes, J.M, Koplan, J.P., "Bioterrorism Preparedness and Response", *JAMA.* 2002; 287:898-900.

7. The White House Report, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", February (2003).

8. Moehle, J.P. (editor). Preliminary Report on the Seismological and Engineering Aspects of the January 17, 1994, Northridge Earthquake, Report No. UCB/EERC 94.01, University of California-Berkeley, January 1994.

9. Viswanathan, S., Eria, L., Diunugala, N., Johnson, J and McClean, C., "An Analysis of Effects of San Diego Wildfire on Ambient Air Quality", Air and Waste Management Journal, 56:56-67 (2005)