Implementation of a Pilot Course at Texas A&M University on Designing Nuclear Security Systems

W.S. Charlton and D.G. Ford
Nuclear Security Science and Policy Institute
Texas A&M University
College Station, Texas 77843

1. Abstract

In 2009, Texas A&M University (TAMU) began working with the Global Threat Reduction Initiative (GTRI) to perform voluntary upgrades to the security systems for the nuclear and radiological materials on campus. Those upgrades were successfully completed and a commitment was made by TAMU to maintain and periodically performance test the security system. As part of the GTRI upgrade process, it became apparent that typical nuclear engineering and health physics curricula do not instruct students on designing and evaluating nuclear security systems. This lack of basic education in this area lengthened much of the GTRI upgrade process since the personnel involved on site had to be educated "on the job". With help from Sandia National Laboratory (SNL), TAMU developed a pilot course on designing and evaluating nuclear security systems which was implemented as an undergraduate course in Spring 2011. The course had 19 students enrolled in it and covered the science and engineering associated with the design, evaluation, and implementation of systems to secure nuclear and radiological materials. The course material included characterization of the adversary, categorization of targets and the consequences associated with failure to protect those targets, detection and delay technologies, on-site and off-site response as well as different response strategies, evaluation of insider threats, mathematical methods for evaluating risk due to the threat and the security system design, and methods for risk minimization. Students completing this course should have a broad picture of nuclear security components and their interconnections into a sustainable nuclear security program.

2. Introduction

"The terrorist attacks on September 11, 2001, reaffirmed the need for collective vigilance, enhanced security, and improved emergency preparedness and incident response capabilities across the Nation's critical infrastructure" [1]. The threat of the malicious use of nuclear and radiological materials (including nuclear terrorism) is growing. On April 12-13, 2010, the United States hosted the first Nuclear Security Summit in Washington D.C., bringing together 49 world leaders in an effort to "discuss steps...to secure loose nuclear materials; combat smuggling; and deter, detect, and disrupt attempts at nuclear terrorism" [2]. As part of the broader nuclear disarmament goals originally outlined in Prague, President Obama convened this group to foster "an international effort to secure all vulnerable nuclear material around the world within four years" [3]. This summit resulted in the production of a Work Plan [4] that outlines the main steps that should be taken to achieve this goal. In addition to encouraging better implementation of existing treaties and programs, the Work Plan urged participating states to more broadly cooperate with international organizations, governments, industries, academic institutions and other stakeholders in an integrated approach to developing the human resources necessary to implement nuclear security measures. Such development would include networking of professionals as well as education and training to establish and maintain an adequate nuclear security infrastructure.

In the U.S., several agencies and organizations have been actively involved in efforts to combat the threat of nuclear terrorism. This includes the U.S. Nuclear Regulatory Commission (NRC) and the National Nuclear Security Administration's (NNSA) Office of Defense Nuclear Nonproliferation. These two agencies work in parallel to achieve this goal:

1. The U.S. Nuclear Regulatory Commission (NRC) has made significant enhancements to the security systems at nuclear power plants throughout the U.S. (as well as security systems for radioactive materials the NRC regulates). However, in order to maintain these security systems and to promote additional security improvements, we must work to forward an enhanced security culture throughout the U.S. and promote the use of technology in security systems. Reaching that goal must include nuclear security technology as a component of the U.S. education system in order to provide a long-term continuous development of nuclear security as a discipline.
2. On May 26, 2004, the NNSA launched the Global Threat Reduction Initiative (GTRI), a collaborative program aimed at securing vast stocks of dangerous nuclear material scattered around the globe. GTRI is achieving its mission through three key subprograms: Convert, Remove, and Protect. These subprograms provide a comprehensive approach to denying terrorists access to nuclear and radiological materials. The GTRI program has been effective in enhancing security; however, in order to ensure the sustainability of these programs, a pipeline of human resources with sufficient education and skills must be provided.

Thus, there is a degree of synergy between the identified need for nuclear security education and the mature agency programs to implement security measures at sites across the globe.

It has been stated by some that the attention to nuclear security education may be the most novel and potentially significant long-term product of the April 12-13 summit. [5] One would be hard-pressed to find any high schools and more than a remarkably few colleges or universities that offer courses that enable students to study the subject of nuclear security. It is largely due to this paucity of course material that the IAEA recently released a set of guidelines on nuclear security education programs. [6] This set of guidelines was developed through consultation with a number of academics from around the world and consists of a suggested course of study for a certificate or a Master of Science degree in nuclear security. The guidelines suggested a number of courses in an effort to provide an educational framework based on a comprehensive approach to nuclear security. That approach goes beyond the traditional area of physical protection at nuclear sites and includes border monitoring, nuclear forensics, consequence management, and other areas.

When studying human capital development needs for nuclear security, three principal needs present themselves:

1. Need 1. New human capital at the entry-level educated in a social or natural science discipline and with an awareness of nuclear security as a possible field of employment and with an understanding of how to approach some problems from a security perspective. These could be individuals with undergraduate or graduate degrees.
2. Need 2. New human capital, at the entry-level, educated in a science or engineering discipline with advanced nuclear security knowledge and who can immediately contribute to specific areas of the nuclear security field. These would likely be individuals with graduate degrees.
3. Need 3. New human capital into the nuclear security field through mid-career transitions from other fields. These individuals enter the field with a detailed knowledge of their previous area but often with little knowledge of the specific details of the field of nuclear security and possibly without an understanding of how to approach problems from a

security perspective. These individuals might have a degree in a supporting discipline but would be served by outreach education and/or continuing education opportunities.

One view of a comprehensive nuclear security approach can be seen in Fig. 1. It is unlikely that any single degree program could cover all of the areas presented in Fig. 1; however, it is possible to formulate a certificate or degree program that could provide a good basis for production of human capital that could be later trained more deeply in specific areas.

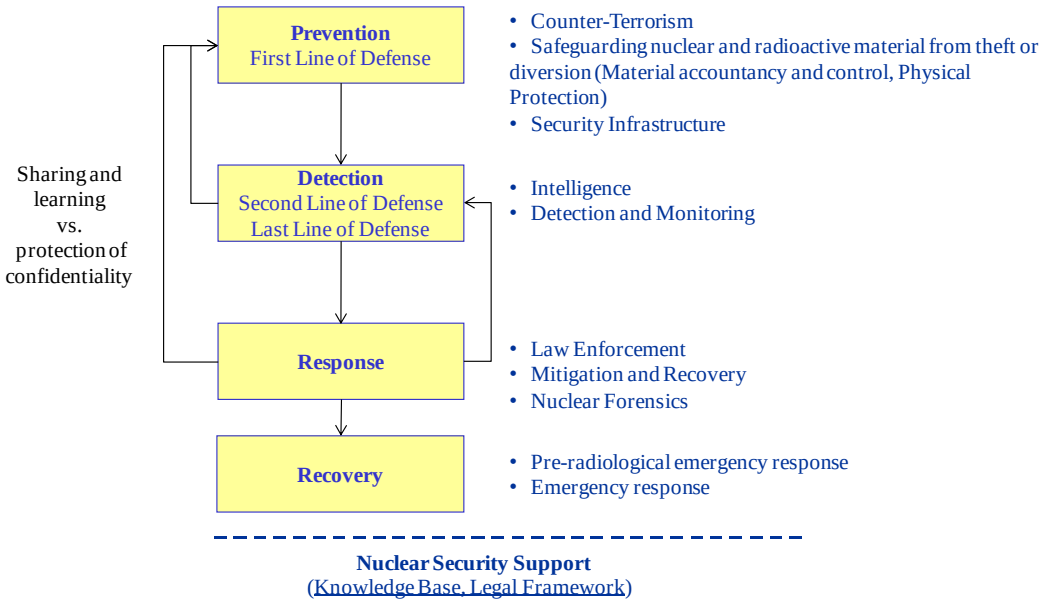

Fig. 1. Comprehensive approach to nuclear security [adapted from a presentation by A. Nilsson (IAEA)].

In this paper, we present a pilot course that was developed and implemented at TAMU to educate students on the design of nuclear security systems that is aimed at meeting the first and second needs presented above. Below we will describe the design of the course as well as the outcomes from its initial implementation.

3. Course Learning Objectives

The primary goal of this course was to educate the student to think with a security perspective such that they can design and evaluate systems to deter, detect, interdict, and respond to threats to the security of nuclear and radiological materials. After completing this course, the student should be able to:

1. Analyze motivations and capabilities of adversaries (terrorists, criminal groups, protestors, etc.).
2. Characterize a threat that can be used to perform a threat-informed security evaluation, including development of a Design Basis Threat (DBT).
3. Assess the limitations and sensitivities of a security analysis using a DBT.
4. Describe and explain the operation of detection, delay, and response technologies. Understand how to complete a performance evaluation of these technologies.

5. Evaluate insider threats to nuclear and radiological facilities (including nuclear power and fuel cycle facilities, research reactors, storage facilities, large industrial radioactive sources in fixed sites, and medical facilities using radiological sources).
6. Incorporate the insider threat in a system design and analyze insider threat scenarios.
7. Formulate different response strategies (including deterrence, denial, containment, pursuit, and recapture) for different facilities and considering on-site and/or off-site response.
8. Use nuclear or radiological material facility characteristics and a DBT to design a performance-based security system for a facility that will be threat-informed, provide defense in depth, and achieve balanced protection while minimizing risk to an acceptable level.
9. Apply engineering principles to produce a cost benefit analysis for upgrade options for an existing nuclear or radiological facility.
10. Describe the limitations of the analysis process, the impact of conservative results, and the sensitivity of results to input parameters.
11. Understand the unique security characteristics associated with transportation of nuclear materials, smuggling of nuclear materials, and protection of major public events and be able to apply a risk- and performance-based engineering approach to security systems for these scenarios.
12. Understand nuclear forensics as a component of a nuclear security system and be able to use nuclear forensics interpretation of measured data to predict infer actor involvement in a nuclear security incident.
13. Discuss and critique the deterrence characteristics of nuclear security systems.

4. Textbooks Used

There are many textbooks that discuss nuclear security and physical protection from a generalist standpoint but few textbooks that were created with an academic approach in mind. For this course, we selected to use the following texts as primary reading materials for the course:

1. Mary Lynn Garcia, *Design and Evaluation of Physical Protection Systems*, Elsevier Science & Technology Books, ISBN 075068352X (2007).
2. Betty E. Biringer, et al., *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*, John Wiley & Sons, Incorporated, ISBN: 0471793523 (2007).

We also used the following additional reading materials:

1. International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225 Rev. 4 (corrected), Vienna (1980). (Available at http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html.)
2. International Atomic Energy Agency, *Amendment to the Convention on the Physical Protection of Nuclear Material*, IAEA International Law Series No. 2, Vienna (2006). (Available at http://www-pub.iaea.org/MTCD/publications/PDF/Pub1275_web.pdf.)
3. International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources*, Vienna (2004). (Available at http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.htm.)
4. International Atomic Energy Agency, *Handbook on Physical Protection of Nuclear Material and Facilities*, IAEA-TECDOC-1276, IAEA, Vienna (2002).

5. International Atomic Energy Agency, *Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage*, IAEA Nuclear Security Series No. 4, Vienna (2007). (Available at http://www-pub.iaea.org/MTCD/publications/PubDetails.asp?pubId=7574.)
6. International Atomic Energy Agency, *Combating Illicit Trafficking in Nuclear and Other Radioactive Material*, IAEA Nuclear Security Series No. 6, Vienna (2007). (Available at http://www-pub.iaea.org/MTCD/publications/PubDetails.asp?pubId=7806).
7. C.D. Ferguson and W.C. Potter, *The Four Faces of Nuclear Terrorism*, Monterrey Institute of International Studies, Monterrey (2004). (Available at www.nti.org/c_press/analysis_4faces.pdf).

5. Course Material

The course was designed to include two 1.5 hour per week lecture and discussion sessions, reading assignments for each session, seven homework assignments, a mid-term exam, and a group design project. The course was designed as a full semester course (14 weeks) and is intended to consume 3 hours of in-class time per week and 6 hours of out-of-class time per week for the students. A brief description of each of these course material components is given below.

5.1 Lectures

The material for the lecture and discussion sessions was developed using the textbooks mentioned above as well as through direct input from experts at Sandia National Laboratory (SNL), Y-12 Nuclear Security Complex, and the U.S. Department of Defense (DoD). The most significant input was provided when faculty and staff from TAMU spent two weeks at SNL in the Summer 2009 participating in an intensive physical protection system training course. These inputs were synthesized and adapted to prepare an educational course that would help to achieve the learning objectives described above. A list of the lecture and discussions sessions used in the course is shown in Table 1. Each lecture session began with a list of discussion questions that were reviewed as a group. This served to help review the material that was covered in the previous lecture and to stimulate thinking amongst the students. Examples of the discussion questions from session 20 are:

1. How does our risk analysis change when assessing risk for low and medium value targets?
2. What conservatisms exist in the process described? How could these be overcome?
3. What characteristics/inputs is this process most sensitive to?
4. Is it more important to have a lower average risk or to have a lower uncertainty in the average risk?
5. How is the overall nuclear security system a “system of systems” approach? How does this aid in reducing our susceptibility to single point failures?

Throughout the course the students were expected to develop an understanding of and ability to assess the following basic functions of a physical security system:

1. Deterrence
2. Detection
3. Delay
4. Response
5. Recovery

Table 1. Lecture Sessions used in Nuclear Security System Design Course.

Session	Lecture
1	Design and Analysis of Security Systems
2	Emerging Threat Characteristics
3	Malicious Uses of Radioactive Materials and Illicit Trafficking
4	Threat Assessment and the Design Basis Threat
5	Facility Characterization and Target Identification
6	Consequence Analysis
7	PPS Performance Objectives
8	Intrusion Detection: Exterior and Interior Sensors
9	Access Control
10	Contraband Detection
11	Field Detection Sensors at Borders/Major Public Events
12	Alarm Assessment, Communication, and Display
13	Access Delay
14	Response and Neutralization
15	Adversary Path Analysis and Multi-Path Optimization
16	Scenario Development
17	Insider Analysis
18	Transportation
19	Design Approaches and Vulnerability Assessments
20	System Design at Major Public Events
21	Design of Security Systems to Interrupt Illicit Trafficking
22	Analysis of Quantitative Risk Assessment Methods
23	Response and Recovery
24	Nuclear Forensics: Part I
25	Nuclear Forensics: Part II
26	Analysis of the Deterrence Value of Security Measures
27	Summary

However, the course focused primarily upon detection, delay, and response since these are the functions that can be most readily performance tested. The course material also was designed to instill upon the students the importance of the following basic design philosophies for any nuclear security system:

1. Defense in Depth
2. Balanced Protection
3. Detection Away from the Target
4. Delay Closer to the Target

The material was developed such that optimal designs for the security systems would reflect these philosophies.

5.2 Readings

The students had assigned readings from the texts that were to be completed before each lecture session. These readings were intended to provide the student with enough background material that they could participate actively in the lecture and discussions. We found that the amount of reading material available that focused on security thinking as opposed to process description was limited.

5.3 Homeworks

Seven homework assignments were generated to allow the students to practice their mastery of the course material throughout the semester. These assignments were due approximately once per week for the first 4 weeks of class and then every other week for weeks 6-10. The homework assignments ranged from simple testing usage of data tables to open source analysis of possible adversaries to performing risk analysis for hypothetical facilities to assessing the capabilities and sensitivities of risk analysis methods.

5.4 Mid-Term Exam

A mid-term exam was conducted in week 9. This provided an opportunity to assess the student's performance with the material. The mid-term focused primarily on understanding of concepts, ability to perform simple calculations, and ability to assess the validity of results. It did not rigorously test the students' security system design capability.

5.5 Design Projects

The course was developed such that the students would have a capstone project for the course which involved a vulnerability assessment of a hypothetical nuclear facility and a re-design to develop upgrade options that will allow the facility to meet a specified allowable risk level. The nuclear facility used in this design project was a small research reactor. The students were given the specifications of the facility and the existing physical protection system in place (detection systems, delay elements, and response force makeup). They worked in small teams (approximately 4-5 students per team to optimize their design) to complete their design. The students would then report their design in an oral presentation and a written report.

6. Implementation and Lessons Learned

This course was taught as a pilot course in the Spring 2011. Nineteen students were enrolled in the course. This included primarily nuclear engineering students but there were also one systems engineering student and one mechanical engineering student in the class. The students were approximately 50% graduate students and 50% upper level undergraduate students.

Feedback from the students on the course was very positive. The students remarked that they would advise other students to take this course. For many of the undergraduate students, this was the first exposure they ever had to a nuclear security topic. This significantly challenged their method of thinking when trying to design a system. These students were used to thinking from a safety and economic perspective when designing systems and had not considered the design from a security perspective (involving an intelligent and adaptable adversary). The students enjoyed the lecture and discussion material and the project the most. They did not find the homeworks or reading materials to be as useful.

The students found that the reading material was too basic and did not have enough technical rigors to demand their attention. They also wanted more reading materials focused on adversary threat assessments.

The students thought that many of the homework assignments were too easy and should be expanded to include more topics. For example, they suggested a future assignment that included an assessment of the interplay between safety and security systems.

All of the students worked on the same facility for their design project. This limited the scope of characteristics that the students were exposed to. The students suggested that in the future we should provide them with four different projects to choose from:

1. Power reactor
2. Research reactor
3. Medical source at a hospital
4. Transportation of radioactive material

These would provide for more overall breadth for their analyses.

The nuclear portions of the course were very demanding for the non-nuclear engineering students. They simply had no familiarity with nuclear physics or radiation detection and it was difficult for them to grasp that material without outside help (which was provided by the instructor in one-on-one help sessions).

The difficulty level of the material was sufficient for upper level undergrads and first year graduate students in nuclear engineering. The math requirements for theft targets were relatively low-level, but the analysis for sabotage targets was significantly more complicated. In the future, additional emphasis on assessments of the risk analysis methods used should be included.

The course also contained too much material to cover effectively. In the future, sessions 24 and 25 (on nuclear forensics) should be moved to a different course.

7. Conclusions

With assistance from the U.S. national laboratories, TAMU developed and implemented a course educating students on designing and evaluating security systems for nuclear and radiological facilities. The course material included characterization of the adversary, categorization of targets and the consequences associated with failure to protect those targets, detection and delay technologies, on-site and off-site response as well as different response strategies, evaluation of insider threats, mathematical methods for evaluating risk due to the threat and the security system design, and methods for risk minimization. Students completing this course should have a broad picture of nuclear security components and their interconnections into a sustainable nuclear security program. This course will help to meet identified needs in human capital within the U.S. and could be implemented at other universities both within and outside the U.S. Student feedback on the course was very positive but also provided an excellent opportunity for updating the course material. This course will be taught again in 2012 after refinement of the material, and once approved by the TAMU administration, it will be institutionalized into the TAMU course catalog.

8. Acknowledgements

The initial development of this course material was supported by a grant from the U.S. Nuclear Regulatory Commission under grant number NRC-38-09-901. Continued development of this material is supported by the Global Threat Reduction Initiative through PNNL contract #156080.

9. References

1. "Protecting Our Nation Since 9-11-01," U.S. Nuclear Regulatory Commission, NUREG/BR-0314, 2004.
2. America.gov, "Press conference by President Obama in L'Aquila, Italy," 10 July 2009, www.america.gov.
3. "Remarks by President Barack Obama, Prague, Czech Republic," 5 April 2009, www.whitehouse.gov.
4. Office of the Press Secretary, "Work Plan of the Washington Nuclear Security Summit," 13 April 2010, www.whitehouse.gov.
5. W. Potter, "Bomb School," Foreign Policy, 23 April 2010, www.foreignpolicy.org.
6. International Atomic Energy Agency, "Educational Programme in Nuclear Security," Nuclear Security Series No. 12, March 2010.