12-36
App - 9/18/12
Senate - App-10/9/12

Undergraduate Distance Education Review Form

(Required for all courses taught by distance education for more than one-third of teaching contact hours.)

Existing and Special Topics Course

Course: CRIM 321 - Cybersecurity and Loss Prevention

Instructor(s) of Record: Dennis Giever

Phone: 724-357-6941 **Email:** dgiever@iup.edu

Step Two: Departmental/Dean Approval

Recommendation: ☒ Positive (The objectives of this course can be met via distance education)

☐ Negative

9/11/12
Signature of Department Designee Date

Endorsed: 9/13/12
Signature of College Dean Date

Forward form and supporting materials to Liberal Studies Office for consideration by the University-wide Undergraduate Curriculum Committee. Dual-level courses also require review by the University-wide Graduate Committee for graduate-level section.

Step Three: University-wide Undergraduate Curriculum Committee Approval

Recommendation: ☑ Positive (The objectives of this course can be met via distance education)

☐ Negative

Gail Sechrist 9/18/12
Signature of Committee Co-Chair Date

Forward form and supporting materials to the Provost within 30 calendar days after received by committee.

Step Four: Provost Approval

☒ Approved as distance education course ☐ Rejected as distance education course

Gerald W. Intemann 9/20/12
Signature of Provost Date

Forward form and supporting materials to Associate Provost.

Undergraduate Distance Education Review Form

Course: CRIM 321 – Cybersecurity and Loss Prevention

Instructor(s) of Record: Dennis Giever

Phone: 724-357-6941 **Email: dgiever@iup.edu**

A. Provide a brief narrative rationale for each of the items, A1-A5.

1. How is/are the instructor(s) qualified in the distance education delivery method as well as the discipline?

   I began my training and work in the area of distance education as a faculty member at New Mexico State University (NMSU). I served as the College of Arts and Sciences representative to the Advisory Committee of Distance Education (1997-1998). While working at NMSU I attended a number of workshops on distance education technology and also teaching techniques for on-line delivery. I have attended numerous workshops at IUP in the areas of on-line instruction, receiving training in WebCT, Moodle, and D2L. I have been active in Reflective Practice as well. The first class I taught on-line was a Special Topic Course in Corrections some 10 years ago. I developed and taught, at the graduate level, our on-line version of CRIM 718 – Quantitative Strategies for Analysis in Criminology. To date I have taught this class three times, and am currently teaching it a fourth time. This class has been very well received by students, and I was asked by IT Support Services to provide a quest lecture outlining my development and delivery of this course. I have been an active member of the Academic Computing Policy Advisory Committee (ACPAC) since 2003, and served as co-chair from 2006 – 2008. I have been a member of the On-Line Action Team since its inception, serving on the committee that evaluated and ultimately selected Moodle as IUP's LMS.

   My efforts in the specific areas related to this class include my work in the area of information assurance, my collaboration with Sandia National Labs, and also my work with the private security sector, including ASIS International and a number of private organizations. During the summer of 2007 I was honored to participate with 35 other individuals throughout the United States in the SHARP program. The SHARP program is a project funded by the Director of National Intelligence which brings together academicians, members of law enforcement, and the intelligence community to solve "hard problems." In fact, SHARP stands for Summer HARd Problem. It is an outgrowth of similar programs involving computer science and a number of hard sciences that have been held each summer since the 1950s. During these programs, scientists have worked on any number of highly classified projects dealing with nuclear proliferation, encryption and others. The summer of 2007 was the first that involved the social scientists, and I was fortunate and honored to be included as one of only four academicians. We spent four weeks in Florida over the summer in a classified environment looking at new ways for the intelligence community to deal with the emerging terrorist threat. It was a once in a lifetime opportunity, and one of which I am very proud to have been a part. I have also worked or consulted with Sandia National Labs during numerous summers addressing physical and cyber security, reviewing and analyzing new technology and their application to emerging threats. I spent two weeks in the summer of 2005 working in one of their testing sites (Area 3) in Albuquerque, New Mexico.

In December of 2000, Mary Micco, Bill Oblitey and I began the process of establishing IUP as one of only about 36 centers of academic excellence in information assurance. This was no small feat. The process involved the writing and subsequent obtainment of a $250,764.00 capacity building grant from the National Science Foundation to both train those working at IUP and equip our laboratories to enter the field of Information Assurance. We had to also develop courses for an interdisciplinary minor in Information Assurance in both Criminology and Computer Science (of which this proposed course is a requirement in the minor). Once the courses were developed and the curriculum process was underway, we applied to the National Security Agency for the distinction of a Center of Academic Excellence. This process was an arduous one involving countless hours completing the necessary application forms and aligning our course work to the National Security Telecommunications and Information Systems Security Standards. More importantly, we brought the IUP community together to meet the rather stringent requirements for any institution that has this distinction. I must point out that when IUP was approved as a center of academic excellence, it brought much publicity to our university. The only other school in Pennsylvania at that time with this distinction was Carnegie Mellon, and other notable schools in the Northeast included MIT, James Madison and George Washington.

2. How will each objective in the course be met using distance education technologies?

The objective of this course will be met utilizing a number of features in the LMS. I will address the specific course objectives first, and then outline other features of this course.

a. Possess an understanding of physical security design and evaluation.

   i. This first objective will be met utilizing a number of techniques including discussion board to review material from the textbook for the class. The class is structured as a set of modules that make up an overall system. An understanding of each module or component is critical to fully understand the entire system. Each discussion board will be monitored and students will be given participation grades in each (to be given at the end of each module, so they can adjust their participation in subsequent modules).

ii. A number of video clips (both of myself briefly explaining a key construct, or showing the testing of some aspect of physical security) will be utilized to provide additional detail to a number of these components.

iii. Each module will have a short quiz which students will take at the conclusion of the module. These quizzes will be designed to test students at higher levels of the learning domains (focusing on their abilities to select the most effective or efficient solutions to problems that are presented).

b. Gain an understanding of the process of evaluating existing or proposed physical protection systems.

i. A number of tools will be given to students to apply their knowledge of existing or proposed physical protection systems that they will utilize to assess a fictitious security facility. Small groups of students (3 to 4) will be required to evaluate this fictitious facility utilizing a software program developed by Sandia National Labs – Estimate of Adversary Sequence Interruption or EASI. This software program will be demonstrated to students with Captivate and, if necessary, a Livescribe lecture. Students will first test the existing facility and develop a baseline. Once this is accomplished, they will make recommendations on upgrades to the facility (changes in policy, upgrades in detection, delay and the response). The final step is to, once again, test the upgraded facility. The goal is for students to gain an understanding of how enhancements to the existing facility (procedures, personnel and equipment) will improve that facility's overall security posture.

ii. The major assignment for the course is a group project which will be the group's recommendation for a facility upgrade. Students will first test the existing fictitious facility – make educated recommendations for facility upgrades – then test this redesigned facility. Improvements in the overall design of the facility are the goal. Each group will turn in a 12 – 15 page paper, printouts from EASI, and drawings of upgrades to the facility.

c. Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might harm them.

i. Entire modules will address policies and procedures. As an example, students will have to deal with "use of force" within their facility. They will be required, within their groups, to write policies on use of force for their response force. Other policies that students will address include, entry control (both humans and equipment), hiring – dismissal of employees, and access control.

ii. Students will also develop policies or MOU's for collaborations with outside agencies (law enforcement, suppliers, and vendors).

d. Recognize the threat from domestic and foreign terrorism.

i. One entire module deals with the threat to their facility. Students will learn to review intelligence reports, police reports and internal documents in the development of a "Design Basis Threat" or DBT. The DBT is the threat that you design your facility against. It comes with the realization that you cannot protect your facility from everything – you must have an awareness of the specific threat to your facility (which can change), and develop strategies, policies and such (a system) to defeat that threat.

   ii. Students will look at examples (case studies) of instances in which a threat assessment was undertaken for a number of facilities (drug manufacturers, airports, border crossings).

e. Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

   i. The final product for this course is the development of an upgrade to a fictitious facility. Students, working in groups, will develop this upgrade and test their design's effectiveness (with a modeling program) against the design basis threat. The final product will include sections from each module in the course (there are 11 total modules).

   ii. Each section will be developed throughout the course, with students and me evaluating each as they are presented. Since the process is system based, it is critical that each step is completed before moving to the next step in progression. Students, as they progress through the system, will gain an understanding of how changes at one level within the system will impact other aspects of the system.

3. How will instructor-student and student-student, if applicable, interaction take place?

   a. Instructor-student interaction will take place through a series of chat rooms, each designed to accomplish the goals of a single module. Students will be required to complete a number of individual projects (short projects to insure understanding of concepts) and group work. Each group (of 3 to 4 students) will complete 11 modules for the course. Those 11 modules will make up the final product for the class. This final product is an upgrade to the security systems for a fictitious facility (see attachment). Not only will I monitor the completion of each module, but students in other groups will have the opportunity to evaluate their peers' products after the due dates.

   b. Student to student interaction will take place in assigned groups – to complete each module and the overall upgrade to the facility. Students will have to work collaboratively on these modules and will be graded on their overall participation (students will also be able to evaluate the contribution, anonymously, of others within their group).

   c. Students in other groups will be required to evaluate and offer suggestions to other groups' products.

   d. Interactions will take place through designed chat rooms, by email, phone calls, Skype and other media (including a number of short video lectures, Captivate lectures and Livescribe lectures). While some interactions will not be monitored, student evaluations will take place in the chat rooms. Students will be advised after each module of their current participation levels, so adjustments can be made throughout the course.

4. How will student achievement be evaluated?
   a. Students will have 11 short quizzes to assess their understanding of key components of the class. These quizzes will focus on a student's ability to select the most appropriate solutions to problems that are presented in that module.
   b. Students will be evaluated after each module and given a participation grade for their input and effort for that section.
   c. There will be five short written assignments during the semester. These assignments will require the students to look at an existing or emerging problem and offer their insights into possible solutions. These critical thinking exercises will include examples such as the recent breach of Kennedy Airport in New York by a stranded jet skier, or the recent intrusion of a nuclear facility.
   d. Students, as a group, will be graded on their overall final product (the final product, overall upgrade to the fictitious facility). Students will be given the opportunity to anonymously assess the contribution of fellow group members.
5. How will academic honesty for test and assignments be addressed?
   a. This is always a concern with on-line instruction. It is my hope that by assessing students in a number of differing fashions, this problem can be reduced. Quizzes will be timed and students will be given a short time frame to respond to each question (you either know the answer or not).
   b. The chat rooms will be evaluated based on the quality of the contribution of each student. Students within these small groups will be working together closely and will have interactions both within the chat rooms, and also by Skype, e-mail and phone conversations.
   c. Students will fill out an honor statement at the beginning of the course (see attached).
   d. During the first module, students will be reminded of academic honesty and how any violation of such a policy can adversely impact their lives in the future (security clearances and such). Many taking such a class will have an interest in the law enforcement or security work, and they will be reminded that any question of their integrity could adversely impact their prospects of gaining employment.

The authors will utilize a large number of possible tools to both enhance this class, and enhance students' understanding of the materials. Each of the tools mentioned above (chat rooms, Captivate, Livescribe, Skype, video files, etc.) have been utilized by the author for existing on-line classes. The only new tool for this class will be a software program developed by Sandia National Labs which will be provided at no cost to the students (it will be demonstrated with Captivate and Livescribe).

SYLLABUS
CRIM 321
Cybersecurity and Loss Prevention
Winter 2013

Instructor: Dennis Giever
Office: G-12 Wilson Hall
Phone: Office: 724-357-6941
Cell: 724-388-9709
E-Mail: dgiever@iup.edu

On-Line Office Hours:	Monday	9:00 – 12:00
	Tuesday	9:00 – 12:00
	Wednesday	9:00 – 12:00
	Thursday	9:00 – 12:00
	Or by appointment	

The instructor's office hours are scheduled for the exclusive use of students. Feel free to utilize this time. At times other than the specified hours you are welcome to call the instructor's office, but you may find that other commitments preclude extended discussions. The instructor believes that informal discussions between students and instructors are an important part of the university experience and, therefore, encourages it through the maintenance of this "open door" policy.

Course Description:

Addresses the cybersecurity threat from a more comprehensive standpoint. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat, to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this course. Students will also be exposed to the private and public responses to computer security problems, including the insider threat, domestic and foreign terrorism, and a number of unique computer crimes and solutions to deal with these crimes. The importance of a sound security policy in the overall management of any organization will be addressed.

Americans with Disabilities Act:

If you have or believe you have a disability, you may wish to self-identify. You can do so by providing documentation to the Disability Support Services (a unit of the Advising and Testing Center). Further information may be obtained in 106 Pratt Hall or by calling (724) 357-4067. Appropriate accommodations may then be provided for you.

Course Objectives:

Upon completion of the course students will:

- Possess an understanding of physical security system design and evaluation.
- Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.
- Recognize the threat from domestic and foreign terrorism.

- Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

Prerequisites:

CRIM 101 & 102

Required Text:

Garcia, Mary Lynn (2008). *The Design and Evaluation of Physical Protection Systems. 2nd ed.* Burlington, MA: Butterworth/Heinemann.

Supplemental reading will be provided on-line.

Course Requirements and Grading:

Attendance:
In accordance with university policy (p. 26 of the 2012-2013 Undergraduate Catalog), students are expected to attend classes regularly. It is difficult for students to comprehend a subject as complex as this unless you review all materials provided.

Students are expected to keep pace with the outline provided. Please remember, you must be an "active" participant in this class to gain knowledge and understanding. "Active" participation means that you don't just go through the motions, but that you actively take notes while viewing the lectures. You should work through problems on your own and practice each assignment until it makes sense to you. Please ask questions! Please challenge yourself! Please work individually and collectively to gain an understanding of this material. Take advantage of the "Forum" to share ideas or to help other students gain an understanding of this complex topic.

Exams:
There will be eleven (11) short quizzes throughout the semester, each worth 10 points. Each quiz will contain questions (critical thinking) from your book, lectures, discussions, and video files.

Class Assignments:
There will be five (5) class assignments during the semester, each worth 7 points. The assignments will consist of short written papers focusing on an existing or emerging security issue.

Problem Solution:
This is a group assignment in which each team (or group) will be required to develop policy, procedures and an upgrade to the security system of an existing facility. Each group will test their facility before and after the upgrades have been undertaken. Each group will turn in a final paper with their recommendations and the final results from their tests. This assignment is worth 100 points.

Class Participation:
Students will be evaluated after each module for their level of participation. Students can earn up to 5 points per module for participation. Participation can take many forms – quality of contribution, timeliness of contribution, leadership, unique ideas, asking and answering questions, paying attention, arguing points, and generally contributing to the chat rooms. It is my hope that each student will keep up with all readings and will be prepared and willing to participate.

Summary and Final Grades:

Five components will contribute to the student's final grade as follows:

Exams – maximum of 110 points
Class assignments – maximum of 35 points
Problem solution – maximum of 100 points
Class participation – maximum of 55 points
TOTAL – maximum of 300 points

Letter Grade Values:

A = 270 – 300 points
B = 240 – 269 points
C = 210 – 239 points
D = 180 – 209 points
F = below 180

Online Etiquette:

Discussion, chat, and e-mail spaces within this course are for class purposes only, unless otherwise stated. Please remember to conduct yourself collegially and professionally. Unlike in the classroom setting, what you say in the online environment is documented and not easily erased of forgotten. The following guidelines:

- Avoid using ALL CAPS, sarcasm, and language that could come across as strong or offensive.
- Read all postings before posting your responses to discussion topics so as to not repeat information.
- Keep chat comments brief and to the point. Use /// to indicate that you are finished sharing your input.
- Focus on one topic at a time when chatting or posting to discussions.
- Remember that unlike in face-to-face learning environments what you say in discussions and chats is documented and available to be revisited. Choose your words and discussion topics carefully.
- E-mail should only be used for messages pertaining to the course. Please refrain from sending forwards, jokes, etc. within e-mail.

Academic Integrity Policy:

Indiana University of Pennsylvania expects a full commitment to academic integrity from each student. This syllabus represents a contract between you and the instructor of this course and that you agree to follow the rules and expectations set up therein. Violations of academic integrity may include:

- Providing or receiving unauthorized assistance in coursework, including papers, quizzes, and examinations.
- Using unauthorized materials and resources during quizzes and tests.
- Possessing course examination materials without the prior knowledge of the instructor.
- Plagiarizing, using papers, dissertations, essays, reports, speeches, and oral presentations, take-home examinations, computer projects, and other academic exercises, or passing off of ideas or facts beyond common knowledge, without attribution to their originators.
- Engaging in behaviors that are disruptive or threatening to others.
- Using computer technology in any way other than for the purposes intended for the course.

Please note that the IUP faculty uses a variety of technologies to check the authenticity of student work. Violations of academic integrity will be handled per IUP's Academic Integrity Policy and Procedures. Failure to comply with the policies and procedures may result in a decrease in grade, involuntary withdrawal from an academic program, suspension, expulsion, or rescission of a conferred degree. IUP's full policy on academic integrity is available in the Undergraduate Catalog under Academic Policies at http://www.iup.edu/registrar.

Reading Assignments and Schedule

Date	Topic	Assignment
Jan. 2	Module One: Facility Characterization	Preface, Chapters 1 & 2
Jan. 4	Module Two: Threat Definition	Chapter 3
Jan. 7	Module Three: Target Identification	Chapter 4
Jan. 8	Module Four: Exterior Intrusion Sensors	Chapter 5 & 6
Jan. 10	Module Five: Interior Intrusion Sensors	Chapter 7
Jan. 11	Module Six: Alarm Assessment	Chapter 8
Jan. 14	Module Seven: Alarm Communication and Display	Chapter 9
Jan. 15	Module Eight: Entry Control	Chapter 10
Jan. 16	Module Nine: Access Delay	Chapter 11
Jan. 17	Module Ten: Response	Chapter 12
Jan. 18	Module Eleven: Analysis and Evaluation	Chapter 13-14
Jan. 21	No Class - Holiday	
Jan. 22	Module Eleven Continued – Risk Assessment	Chapter 15 -16
Jan. 23	**Final quiz – Turn in Final Paper**	

Technical Support:

For questions regarding Desire2Learn and using the system, contact the 24/7 Perceptis Helpdesk at 1-877-730-6229 or via the Web at http://smartipantz.perceptis.com/Indiana.

To obtain technical support for computer issues related to this course, please contact Indiana University of Pennsylvania's IT Support Center at 724-357-4000, Monday–Friday, between 7:30am and 5:30pm Eastern Time (ET). You should be prepared to give specific details regarding your technical issue(s), including what you were doing before the error occurred and the exact text of any error messages received. If you experience issues outside of the normal helpdesk hours, you can also submit your error via e-mail at it-support-center@iup.edu or via electronic form available online at http://www.iup.edu/itsupportcenter/help.

SYLLABUS OF RECORD

I. Catalog Description

CRIM 321 Cybersecurity and Loss Prevention	3 lecture hours
Prerequisite: CRIM 101 or CRIM 102	0 lab hours
	3 semester hours
	(3c-0l-3sh)

Addresses the cybersecurity threat from a more comprehensive standpoint. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this course. Students will also be exposed to the private and public responses to computer security problems, including the insider threat, domestic and foreign terrorism, and a number of unique computer crimes and solutions to deal with these crimes. The importance of a sound security policy in the overall management of any organization will be addressed.

II. Course Objectives

Upon completion of the course students will:

- Possess an understanding of physical security system design and evaluation.
- Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.
- Recognize the threat from domestic and foreign terrorism.
- Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

III. Detailed Course Outline

A. Design and Evaluation of Physical Protection Systems (2 Weeks)

Facility Characterization
Threat Definitions
Target Identification

B. Physical Protection System Design (3 Weeks)

The Outsider Threat
Exterior Intrusion Sensors
Interior Intrusion Sensors
Alarm Assessment
Alarm Communication and Display
Entry Control
Access Control
Access Delay
Response

The Insider Threat

C. Analysis and Evaluation (2 Weeks)

Computer Model for Analysis
Risk Assessment

MIDTERM

D. Terrorism (4 Weeks)

History
Federal Response
Weapons of Mass Effect
Chemical
Biological
Cyber
Radiation
Explosives
Crime Scene Operation

E. Cyber Crime (3 Weeks)

Digital Evidence
CyberStalking
Computer Crackers
Forensic Science and Computers

IV. Course Evaluation Methods

Midterm Examination	20%

Final Examination	20%
Review Essays	20%
Final Problem Solution	30%
Attendance	10%
Total	100%

Grading Scale:	90% – 100%... A
	80% – 89%.... B
	70% – 79%.... C
	60% – 69%.... D
	Below 60%.... F

Examinations: There will be two examinations in this class, a midterm and a final. Both will cover material from the books, readings placed on reserve, guest lectures, films and class presentations.

Attendance Policies: Students are expected to attend class regularly, and to prepare for class by reading the scheduled assignments. Since students will be working in groups and sharing their ideas with fellow students, class participation is very important. Students who fail to come to class prepared or have more than 3 hours of unexcused absence can expect to have points automatically deducted from this part of their grade. Students can expect to loss points equivalent to 1% of their final grade per class hour missed due to unexcused absences (remember this is after 3 class hours are missed). If it becomes apparent that a student is unprepared for class, it will be treated as an unexcused absence. Class attendance and participation will be worth up to 10% of your final grade.

Review Essays: Students will be assigned two research essays during the semester. These two research essays will deal with computer security issues within an organization. Students are to critique the article and, utilizing knowledge gained from this class, address a more appropriate method of minimizing the threat.

Final Problem Solution: The final requirement for this class will be a problem solution comprised of two parts – an in class presentation of your system design (10% of your final grade) and a 30 page (minimum) paper describing the new design (20% of your final grade). Students will work in teams assigned by the instructor.

V. Textbooks and Other Required Readings

Garcia, Mary Lynn (2001). *The Design and Evaluation of Physical Protection Systems.* Boston, MA: Butterworth-Heinemann.

Maniscalco, Paul M. & Christen, Hank T. (2001). *Understanding Terrorism and Managing the Consequences.* Upper Saddle River, NJ: Prentice Hall.

Material placed on reserve in the library.

VI. Special Resources Requirements

Existing Cybersecurity Laboratory – Purchased with NSF Grant # 0113533

VII. Bibliography

Casey, Eoghan (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego, CA: Academic Press.

Cooper, Paul (1996). *Introduction to the Technology of Explosives (2nd Ed.).* New York, NY: Wiley.

Dr. K (2000). *A Complete Hacker's Handbook: Everything You Need To Know About Hacking in the Age of the Web.* London, UK: Carlton.

Fennelly, Lawrence J. (1996). *Handbook of Loss Prevention and Crime Prevention (3rd Ed.).* Boston, MA: Butterworth-Heinemann.

Hudson, David (1997). *Rewired: A Brief (and Opinionated) Net History.* Indianapolis, IN: Macmillan Technical Publishing.

Moore, James (2001). *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency – The Bureau of Alcohol, Tobacco, and Firearms.* Urbana, IL: University of Illinois Press.

Nichols, Randall K., Ryan, Daniel J., Ryan, Julie J. C. H. & Coviello, Arthur W. Jr. (1999). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves.* New York, NY: McGraw-Hill.

Pipkin, Donald L. (2000). *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ: Prentice-Hall.

Power, Richard (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Indianapolis, IN: QUE.

Rubin, Aviel D. (2001). *White-Hat Security Arsenal: Tackling the Threats.* Boston, MA: Addison-Wesley.

Simonsen, Clifford E. & Spindlove, Jeremy R. (2000). *Terrorism Today: The Past, The Players, The Future.* Upper Saddle River, NJ: Prentice Hall.

COURSE ANALYSIS QUESTIONNAIRE

Section A: Details of the Course

A1 How does this course fit into the programs of the department? For what students is the course designed? (majors, students in other majors, liberal studies).

This course is designed as one of nine required courses for an interdisciplinary minor in cybersecurity. It will most likely be restricted to students enrolled in the minor.

A2 Does this course require changes in the content of existing courses or requirements for a program? If catalog descriptions of other courses or department programs must be changed as a result of the adoption of this course, please submit as separate proposals all other changes in courses and/or program requirements.

No

A3 Has this course ever been offered at IUP on a trial basis (e.g. as a special topic)? If so, explain the details of the offering.

No

A4 Is this course to be a dual-level course? If so, what is the approval status at the graduate level?

No

A5 If this course may be taken for variable credit, what criteria will be used to relate the credits to the learning experience of each student? Who will make this determination and by what procedures?

This course cannot be taken for variable credit.

A6 Do other higher education institutions currently offer this course? If so, please list examples.

None that we are aware of.

A7 Is the content, or are the skills, of the proposed course recommended or required by a professional society, accrediting authority, law or other external agency? If so,

please provide documentation. Explain why this content or these skills cannot be incorporated into an existing course.

Universities are being encouraged to develop programs in information assurance by the federal government. This interdisciplinary minor is our unique approach to this initiative.

Section B: Interdisciplinary Implications

B1 Will this course be taught by one instructor or will there be team teaching? If the latter, explain the teaching plan and its rationale.

This course will be taught by one instructor.

B2 What is the relationship between the content of this course and the content of courses offered by other departments? Summarize your discussions (with other departments) concerning the proposed changes and indicate how any conflicts have been resolved. Please attach relevant memoranda from these departments which clarify their attitudes toward the proposed change(s).

This course ties directly to the content of other courses in the interdisciplinary minor.

B3 Will seats in this course be made available to students in the School of Continuing Education?

Yes.

Section C: Implementation

C1 Are faculty resources adequate? If you are not requesting or have not been authorized to hire additional faculty, demonstrate how this course will fit into the schedules of current faculty. What will be taught less frequently or in fewer sections to make this possible?

Yes. This course will be taught as part of our electives package. As such, this new course will replace an existing section of another criminology elective class.

C2 What other resources will be needed to teach this course and how adequate are the current resources? If not adequate, what

plans exist for achieving adequacy? Reply in terms of the following:

***Space**

***Equipment**

***Laboratory Supplies and other Consumable Goods**

***Library Materials**

***Travel Funds**

Funds for equipment and laboratory supplies are provided for by an NSF grant.

C3 Are any of the resources for this course funded by a grant? If so, what provisions have been made to continue support for this course once the grant has expired? (Attach letters of support from Dean, Provost, etc.)

Yes. Start up money for course development was provided by an NSF grant.

C4 How frequently do you expect this course to be offered? Is this course particularly designed for or restricted to certain seasonal semesters?

At least once yearly, but as demand increases we may offer this course once a semester.

C5 How many sections of this course do you anticipate offering in any single semester?

One.

C6 How many students do you plan to accommodate in a section of this course? Is this planned number limited by the availability of any resources? Explain.

We plan to accommodate 30 students in each section offered.
No.

C7 Does any professional society recommend enrollment limits or parameters for a course of this nature? If they do, please quote from the appropriate documents.

No.

Section D: Miscellaneous

Include any additional information valuable to those reviewing this new course proposal.

Honor Statement

The following is an example honor statement. You can present this statement or one similar to it at the beginning of the class to serve as evidence that the student has read the syllabus and agreed to the course policies. Some learning management systems allow you to set release conditions based on quiz results. This means a student will able to access the course materials on which the release the condition is set until only after her or she has agreed to the honor code statement.

Additionally, the feedback features in the quiz can be used to provide directions to the student upon completion of the honor statement. For example, a student committing to the course policies may be provided with feedback welcoming him or her to the course. Likewise, a student who does not commit to the course policies may be given feedback to contact the instructor for guidance about how to proceed.

I understand that the syllabus represents a contract between the professor of this course and myself. I have read the syllabus for this course and understand my expectations and the course policies, including those regarding grading, course participation, and academic integrity. I also understand that the professor has the right to alter the syllabus as dictated by the needs of the course. By responding to this post, I affirm that I understand the course rules and policies and that I have been given the opportunity to ask questions.

A. I understand and COMMIT to abide by the policies set forth in the syllabus and course policies.

Feedback: Welcome to [course name]. You may proceed through the course.

B. I DO NOT COMMIT to abide by the policies set forth in the syllabus and course policies.

Feedback: You have indicated that you do not agree with the course policies. You should contact your professor immediately with your questions or further guidance on how to proceed.

CRIM 321

Winter Session 2013

Module One Outline

- Students will read the preface, Chapters one and two in the Garcia book.
- Students will read the on-line *Physical Protection System Design – Exercise Data* handout.
- Students will watch the short video clip on Chapter one.
- Students will watch the short video clip on Chapter two.
- Students will participate in general chat rooms on the readings.
  - I will post discussions on the following topics
    - What are some differences between security and safety?
    - What is meant by integration of technology, people, and procedures to meet protection objectives?
    - Why is deterrence considered secondary and not discussed in the book? Do you agree or disagree with the author?
    - Why is it best to place delay near your target? Why not slow your adversary down further from the target?
    - Does the risk equation make sense to you? Discuss its meaning.
    - In looking at your Exercise Data handbook, what are some general observations and concerns about the Hartley Hub and the secure cargo area?
    - I will also provide an open forum for students to post any ideas or questions from the material in this module.
- Students will work, as a group (3 to 4 fellow students) on the following assignment. Chat rooms will be set up and monitored for each group – each student will be assigned points for their participation in the group chat room as well as the general chat rooms for each module: 0 points for little or no participation – 5 points for superior participation:

> Based on the information provided in the Physical Protection System Design – Exercise handout, you, as a group, must determine what asset you are holding and protecting in the Hartley Hub secure cargo facility. There are a number of important considerations when determining your asset. First, it should be based on the scenario introduced in the handout. Second, be realistic. You do not want to house nuclear material in such a facility as the U.S. Federal Government (Department of Energy) has very specific guidelines (regulations) for warehousing nuclear material. Plus, your decision now will have an impact on your overall design throughout the semester. Develop a realistic asset that would be of value (if they were able to steal) to a possible threat to your facility. Please remember, your next assignment will be to develop what is called a "Design Basis Threat." Your group will be required to determine the most likely threat to your facility, once again, based on the materials gleamed from your Exercise handout. Please write this assignment out as a one to two paragraph description of the asset. This assignment will become part of the final "Problem Solution" for the class. One goal

of each assignment will be to integrate the assignment with the overall "Problem Solution" which will be due at the end of the semester.

Students will not be graded on this assignment (it is part of the bigger, overall final paper for the course). The only points associated with this first assignment will be participation points. The goal is to offer feedback (both by me and other groups), suggestions, and comments to help improve the overall final product.

- Students will take a short timed quiz.

1. Of the following responses, which, according to your text, best describes a Physical Protection System?
    a. A group of components working together to protect your facility.
    b. Integrated subsystems working in coordination to accomplish a single goal.
    c. The integration of people, procedures and technology to meet protection objectives.
    d. The affective functioning of multiple components to meet your security goals.
2. True or False – Safety and security functions deal with pretty much the same issues and concerns.
3. True or False – Security designers should place a lot of emphasis on deterrence when designing their security system.
4. Which of the following is correct?
    a. Detection, Delay, and Response
    b. Delay, Detection, and Response
    c. Response, Detection, and Delay
    d. Reinforce, Detection, and Delay
5. Which one of the following statements is not true?
    a. Detection without assessment is not detection.
    b. A physical protection system performs better if detection is as far from the target as possible.
    c. A physical protection system performs better if delay is as far from the target as possible.
    d. A well designed system exhibits balanced protection.

- The first class assignment will be given (students will have two days to submit their reaction paper). Students will be asked to write a short reaction paper to an article "Port Authority Probes JFK Security Breach by Jet Skier" – or "Security at JFK Breached by Swimmer." They will be asked to think about what went wrong with the new $100 million security system at JFK. From their somewhat limited knowledge at this point in the semester, they will be asked to describe ways that we might improve security at the airport?
    - The goal is to point out flaws in their assessments – which should be numerous at this point in the class. The goal is to provide them with feedback on where they will learn that their ideas might be misguided – for example, a common reaction will be to

increase the number of security personnel to more closely monitor the perimeter of the airport. Students will learn in modules four and six that humans are terrible at detection (we get bored easily and will miss a lot). They will be introduced to an entire section on exterior intrusion detection and how it should be integrated with human alarm assessment (humans do an excellent job of assessing whether a sensor has detected an intrusion or whether a nuisance alarm has taken place – they just don't do well with detection).

CBS 2HD 1055 WCBS 1010 WINS WFAN
New York

FOLLOW US

Search 72°

Buy Tickets Order Food More LOGIN | REGISTER

Home News Sports Best Of NY Events Health Video Audio Traffic Weather Places Deals Autos

News Home New York New Jersey Connecticut Business Politics Health Entertainment Photo Galleries Text Alerts

NEWS

Port Authority Probes JFK Security Breach By Jet Skier

Daniel Casillo Faces Trespassing Charge; PA Has Many Unanswered Questions

August 13, 2012 11:58 PM

Share this Like 92 21 3 42 View Comments

Log In Share CBS Local with your friends. Add us to your Timeline What's this?

FILE – An aerial view of John F. Kennedy Airport (Photo by Spencer Platt/Getty Images)

NEW YORK (CBSNewYork) – A $100 million security system at John F. Kennedy Airport was tested and failed.

Now, authorities are trying to figure out how a man was able to approach the runway in the dark of the night without ever being noticed.

Hundreds and hundreds of hockey-puck sized sensors detect movement on the fence around JFK Airport, which is constantly monitored by dozens and dozens of security cameras. The system, made by defense contractor Raytheon Co., is meant to be a safeguard against terrorists.

1010 WINS' Steve Sandberg reports

It cost millions and millions of dollars, but the detection system failed to detect Daniel Casillo on Friday night when he climbed the fence and entered the airport from the waters of Jamaica Bay.

"I think it's really uncharacteristic of airport security," traveler Lauren Mayernik told CBS 2's Sean Hennessey on Monday night.

Investigators believe Casillo, a 31-year-old from Queens, was riding a Sea-Doo personal water craft with a group of friends. As they raced around bay near JFK, Casillo's machine died and he was left behind.

Desperate for help, he swam towards the lights of JFK, climbed right over the 8-foot-high security fence and crossed two active runways, CBS 2's Tony Aiello reported.

Filed Under

Heard On 1010 WINS, WCBS, WFAN, Local, News, NY News, Watch + Listen

Related Tags

Daniel Casillo, Delta Airlines, Dick Brennan, Isaac Yeffet, jet skier, JFK, JFK Airport, Peter Haskell, Port Authority, Sean Hennessey, Steve Sandberg

Facebook Activity

Read, share and discuss! Add CBS New York to keep your friends up-to-date on the latest local news, traffic and weather.

Log In

Login You need to be logged into Facebook to see your friends' recent activity.

Packing Heat: Statistics Show Number Of Female Gun Owners On The Rise - CBS New York
38 people recommended this.

Facebook social plugin

"I think he panicked, he swam for shore and the first shore he got to was JFK," said Marie Rizzo of Howard Beach.

The Perimeter Intrusion Detection System apparently did not alert and Casillo, reportedly soaking wet and wearing a bright yellow life vest, wasn't spotted until he got all the way to Terminal 3.

WCBS 880's Peter Haskell reports

Casillo has been charged with criminal trespass, according to a complaint. His cousin said he had no choice but to swim to shore and look for help.

"I think it's pretty ridiculous if you ask me," Angelo Casillo told CBS 2's Dick Brennan. "I have no words for it."

Attorney John Ragano represents Daniel Casillo and said "He won't have any comment until he has his day in court and he's really not in good shape in terms of his anxiety at this point."

The Port Authority said it is looking into the matter, adding that it has increased patrols on the ground and in the water .

"We have called for an expedited review of the incident and a complete investigation to determine how Raytheon's perimeter intrusion detection system — which exceeds federal requirements — could be improved," the agency said in a statement. "Our goal is to keep the region's airports safe and secure at all times."

The Port Authority Police union told CBS 2's Hennessey the security breach proves what they've been saying for years.

"The technology's not working," said the PBA's Paul Nunziato. "The system doesn't work. It might work on some sections but it obviously din't work on this section."

But security experts like Isaac Yeffet said they aren't interested in the finger pointing.

"Why we allow ourself to spend millions of dollars and not to have security?" he said. "The bottom line – did we fail? yes or no?"

The security breach also prompted outrage from Sen. Chuck Schumer.

"We've been warning about this real danger for years," Schumer said. "Maybe this is a blessing in disguise that will finally get the Port Authority to do a top-to-bottom investigation of their perimeter security and fix the problems immediately."

Meanwhile, many who live near JFK said they were concerned about what happened.

"They need to pay more attention, especially if they are spending $100 million," Queens resident Christopher Bermudez said.

"It makes me feel unsafe to be quite honest with you," added Eddie Garcia.

Casillo has a court date set for October.

VIDEO NEWS

Mobile Couch – NYC's Best Cookies Part...

More Videos

FOLLOW CBS NEW YORK

Follow @CBSnewyork 19K followers

CBS New York on Facebook

Like 19,736

Free In NYC
Events for lovers of the arts, outdoors and more. We rounded up our favorite freebies in the city this summer.

Best FroYo
Cool down! These are the city's nine best options for your frozen yogurt fix.

WiFi Parks
WiFi is available in many of the city's public parks. Here are 7 outdoor Internet-ready hot spots.

Gluten Free Food
Our latest picks for the best gluten-free menus, desserts and bake shops in NYC and the Tri-State area.

post-gazette.com
Pittsburgh Post-Gazette

Security at JFK breached by swimmer

August 14, 2012 12:00 am
By Meghan Barr / The Associated Press

NEW YORK -- In an era when airline passengers can't get past a checkpoint with a shampoo bottle, security experts were shocked Monday by the case of a man who swam ashore, scaled a fence and walked dripping wet into Kennedy Airport, despite a $100 million system of surveillance cameras and motion detectors.

"Thank God it wasn't a terrorist, but we have to look at it as if we had another attack," said Israeli airline El Al's former security chief, Isaac Yeffet. "That's the only way we'll improve the system."

The Port Authority of New York and New Jersey, which oversees the airport, quickly added police patrols to the airport perimeter and said it is investigating the security breach.

Authorities said the trouble began Friday evening, when 31-year-old Daniel Casillo's jet ski ran out of fuel in Jamaica Bay. He swam toward the bright lights of Kennedy's runway 4L, which juts out into the bay, then climbed an 8-foot fence that is part of the airport's state-of-the-art Perimeter Intrusion Detection System, authorities said.

Soaking wet, wearing a bright yellow life jacket, Mr. Casillo made his way across two intersecting runways -- an estimated distance of nearly two miles -- before he was spotted on a terminal ramp by an airline employee, authorities said. According to the police report, Mr. Casillo told an officer: "I needed help!"

The intrusion-detection system, manufactured by defense contractor Raytheon Co., should have set off a series of warnings, said Bobby Egbert, spokesman for the Port Authority police officers union. "This system is made specifically for those types of threats -- water-borne threats," Mr. Egbert said. "It did not detect him climbing over a fence. It did not detect him crossing two active runways."

Port Authority police questioned Mr. Casillo and charged him with criminal trespassing. Authorities said the airport grounds were clearly marked with no-trespassing signs, indicating that it is a "restricted area for authorized personnel only."

Mr. Casillo was released without bail for a court appearance Oct. 2. A man who answered the phone at the home of Mr. Casillo's girlfriend said the couple's lawyer had advised them to stop speaking to the media.

"We have called for an expedited review of the incident and a complete investigation to determine how Raytheon's Perimeter Intrusion Detection System -- which exceeds federal requirements --

could be improved," the Port Authority said in a statement. The agency offered no explanation of what went wrong, or whether it was human error or equipment failure. A Raytheon spokesman would not comment.

"The catastrophic failure was that nobody sounded the alarm to go to condition-red intruder alert," said former New York City Detective Nicholas Casale, who was the metropolitan area transit agency's deputy director of security for counterterrorism.

"Immediately, there should've been an armed response," he said. "Heavy weapons, armored cars to the area that the perimeter was breached. The airport should have been locked down."

The intrusion-detection system employs sensors, motion detectors and video surveillance, said the Port Authority police union's Mr. Egbert. A security guard employed by a private contractor is supposed to watch the footage from a monitoring room, the union spokesman said. If the guard decides there is a threat, a private security officer is sent to investigate, Mr. Egbert said.

From there, it is up to the private security force to decide whether to notify Port Authority police, Mr. Egbert said.

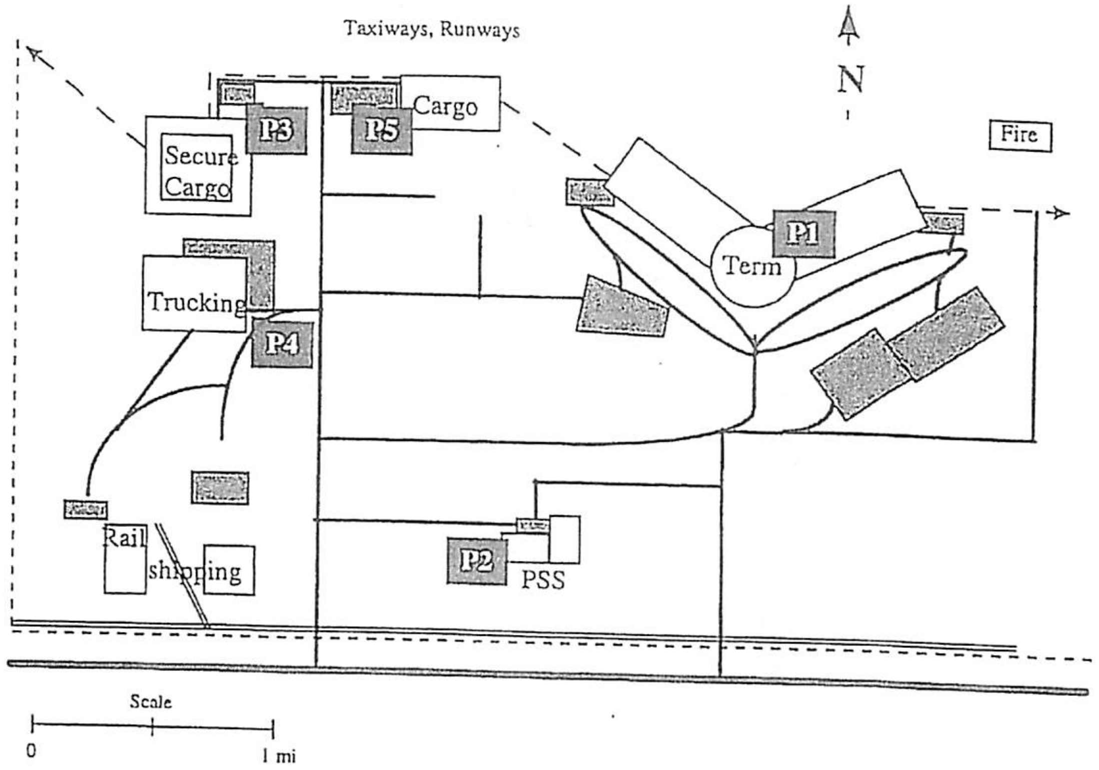
The detection system, which was phased in several years ago, has been a source of tension between the Port Authority and the police union. The union contends that manpower -- in the form of patrols in the air, on the water and on the ground -- is the best way to protect the airport.

"This has all been structured to remove the police from the situation," Mr. Egbert said. "Technology doesn't catch terrorists. Boots on the ground do."

First Published 2012-08-14 00:02:49

Physical Protection System Design – Exercise Data

Hartley International Transportation Hub—Protective Force Locations



═ - Railroad tracks

— — — - chain link fences

- - - - - site boundary

—— - site roads

▬ - major highways

□ - Security Fences

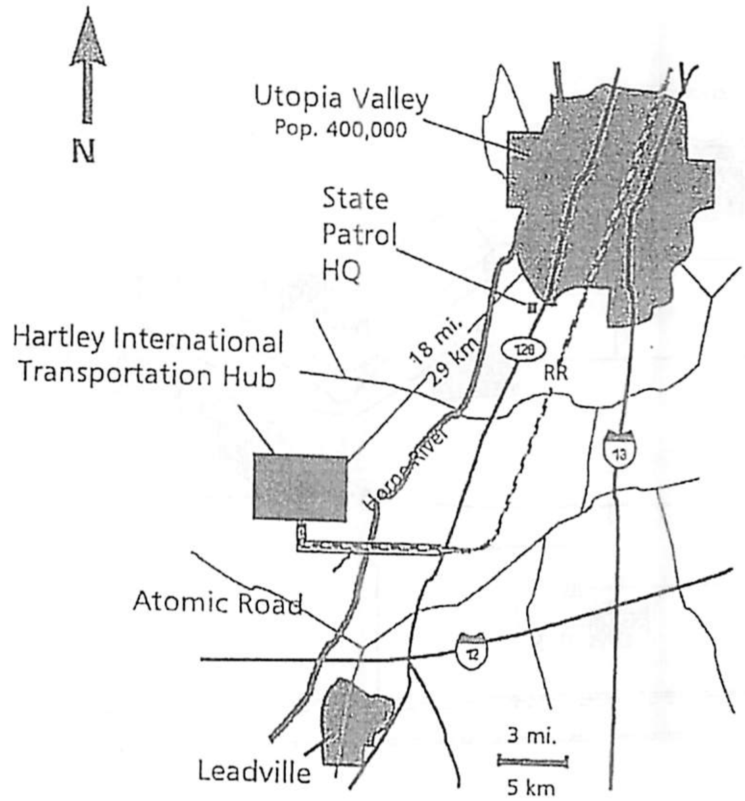
▨ - Parking

P1 - P5 - Protective force stations (P2 is protective force headquarters)

PSS - Police substation

Term - Airport Terminal

Hartley International Transportation Hub



Secure Cargo Area Facility Operation

It is the year 2010. The Hartley Transportation Hub (Hartley Hub) is located in a medium-sized city in the southwest United States. It contains an airport, a rail cargo center, a trucking center, an air cargo terminal, and a secure cargo area. Also located at the Hartley Hub is a police substation. Each of these areas has a security force associated with it.

The Secure Cargo Area (SCA) is open every weekday from 5 AM until midnight; it is closed on weekends. The facility is meant to be a temporary storage location for various high value or critical assets, such as prototype microelectronics, precious metals or gems, drugs seized as evidence or money being taken out of circulation. Hazardous biological agents, such as anthrax, suspected Ebola virus samples and limited quantities of some radioactive substances are stored in a special controlled room. The SCA is protected by a physical security system as shown in the following pages. **Unless specifically noted, drawings are not to scale.**

During normal operating hours, the security force at the SCA consists of three security officers, who are stationed at the front entrance. One officer operates the central alarm system, another is stationed inside the personnel entry, and the third officer mans the vehicle entry portal. When the facility is closed, there are two officers on duty (one operating the central alarm system and the other on random patrol.) Anyone entering the SCA must pass through a personnel portal. Entering personnel first go to a badge exchange window where they exchange a plastic laminated identity badge for a facility access badge, that includes a magnetic stripe and a picture. After the badge exchange, personnel pass through a metal detector and then an explosives detector. The security officer stands by the wall between the two detectors to verify that all persons pass through both detectors. The metal detector is always on. The explosives detector is used on a random basis or when there are hazardous agents stored in the controlled room. After passing through the two detectors, people exit through a set of double doors into the protected area of the facility.

All entering vehicles are searched via in the vehicle portal. This portal consists of automatic sliding gates built into the inner and outer fences surrounding the SCA and is manned by a security officer who conducts a thorough search of the vehicle. Once the vehicle has entered the portal, the driver exits the portal through the open outer gate and enters the SCA through the personnel portal. The officer manning the alarm station then closes the outer gate, thereby, "trapping" the vehicle in the portal until it is cleared to enter. Once the vehicle is searched, the inner gate is opened and the driver, who was cleared through the personnel portal, rejoins the vehicle. All vehicles admitted through the portal must have an entry sticker on their front windshields. If the entering vehicle is picking up or delivering cargo to the SCA, the officer assigned to the portal gets in the vehicle with the driver to go to the staging area.

The Staging Area of the SCA is accessed through a standard roll-up door which is large enough for a vehicle to pull through. The officer and driver exit the vehicle and facility personnel unload the cargo, place the material in the incoming staging section, and complete the required paperwork. The process is reversed for the removal of material from the facility. During operating hours the roll-up door is open and unlocked and the balanced magnetic switch on the door is placed in "access", preventing it from detecting any entry. When the staging is complete, the officer and driver re-enter the vehicle, drive back to the vehicle portal, wait for the inner gate to be opened by the officer at the alarm monitoring station and park the vehicle in the trap. At this time, the officer exits the vehicle, the inner gate is closed, the outer gate is opened, and the driver and vehicle are free to leave the facility. This process is repeated for each vehicle moving cargo in or out of the facility, one at a time.

The Cargo Storage Building at the SCA includes the Office Area, the Vault Area, and the Staging Area. The Office Area is an administrative building where various facility personnel have offices and paperwork for the site is handled. There is also a small lab for maintenance, storage, and repair of small equipment items. Located inside the Vault Area is a Controlled Room, which holds biological, chemical, and radiological samples.

Material at the SCA is stored in a Vault Area which is comprised of a series of steel mesh storage cages of varying size. The Vault Area may be accessed through one of two entry doors. One door is located right off the Staging

Area. The other door is located between the Office Area and the Vault Area. This door is equipped with electronic locks that are opened through the use of a magnetic stripe badge reader and a hand geometry unit. No material is allowed through this door (all material must enter through the Staging Area). The Controlled Room is accessed via the Vault Area and holds environmental chambers for the storage of biological and radiological assets. The chambers can regulate temperature, humidity, and pressure to store these samples appropriately.

There are approximately 60 employees at the SCA. This workforce includes a Facility Manager, a Security Manager, an Operations Manager, engineers and technicians, material handlers, clerks, secretaries, custodians, and security officers. Various subcontractors are also allowed into the facility at times to do maintenance or emergency repair work on heating, cooling, plumbing systems, computers, forklifts, copy machines, etc.

The primary response force for the SCA is the local police, with headquarters at R2 (see map on page 1.) The local police are also responsible for protecting the airport, other facilities at Hartley Hub, and patrolling other areas of the city. As a result, their response time to an attack on the SCA is 20 minutes. When alerted by the dispatcher that the SCA is under attack, all eight police officers on patrol in the city return to headquarters. The first four police officers to reach headquarters become the response force to the SCA, others are released back to normal patrol. These four officers collect their gear, review tactics and procedures, then go to the SCA as a group. Once at the SCA, they contact the local SCA security officer in charge and deploy according to a set procedure.

Table 1. Hartley Transportation Hub—Physical and Environmental Conditions

Topography

The Hartley Transportation Hub is located in the semi-arid southwestern United States on a flat plain. The climate is very similar to Albuquerque, New Mexico.

Vegetation

Small shrubs and grass are the only vegetation allowed to grow near and on SCA grounds.

Wildlife

Small animals such as rabbits, squirrels, dogs, and cats inhabit the Hub. Birds of all sizes are also present.

Background Noise

Seismic disturbances may be caused by railways that are located at the Hub. Some noise may also occur because of heavy passenger vehicle traffic and low-flying aircraft.

Climate/Weather

See Table 2.

Table 2. Hartley Hub—Annual Weather Data

Month	Temperature °C							Degree days Base 18.3 °C		Precipitation in centimeters						Relative humidity %			
	Averages			Extremes						Water equivalent			Snow, ice pellets						
	Daily maximum	Daily minimum	Monthly	Highest	Date	Lowest	Date	Heating	Cooling	Total	Greatest in 24 hours	Date	Total	Greatest in 24 hours	Date	Hour 05	Hour 11	Hour 17	Hour 23
																	(Local time)		
JAN	6.2	-5.3	0.5	13	12	-13	30	549	0	2.72	1.80	17-18	6.6	6.1	25	74	54	45	65
FEB	12.9	-2.8	5.1	23	14	-8	4	369	0	1.57	0.76	16-17	15.2	7.6	16	70	47	31	58
MAR	17.9	0.3	9.1	24	8	-6	5	283	0	0.36	0.18	28-29	Trace	Trace	14	59	32	25	48
APR	23.1	4.6	13.8	29	15	-4	13	134	3	0.61	0.28	9-10	1.3	1.3	3	53	25	17	37
MAY	25.8	9.3	17.6	32	6	2	11	56	37	6.30	2.16	20	2.5	2.5	3	62	34	28	48
JUN	31.7	14.2	22.9	39	28	7	9	6	149	2.59	2.06	8	0.0	0.0		54	27	22	41
JUL	35.6	18.3	27.0	41	14	12	2	0	273	2.03	1.52	16-17	0.0	0.0		52	28	22	40
AUG	32.7	17.3	25.1	38	2	13	20	0	212	3.89	1.98	9-10	0.0	0.0		60	35	25	44
SEP	30.7	14.1	22.4	38	5	8	16	13	138	1.02	0.51	14-15	0.0	0.0		56	32	24	44
OCT	25.6	7.1	16.4	33	5	-3	31	82	25	0.69	0.46	21	2.3	2.3	30	50	26	18	37
NOV	12.1	-2.2	5.0	22	4	-9	29	397	0	2.31	1.88	7-8	2.0	2.0	23	69	41	37	56
DEC	11.3	-5.1	3.2	17	3	-9	31	467	0	2.21	1.83	26-27	6.9	6.4	26-27	66	44	40	57
YEAR	22.2	5.8	14.0	41	JUL 14	-13	JAN 30	2356	838	26.29	2.16	MAY 20	36.8	7.6	FEB 16	60	35	28	48

Table 2. Hartley Hub—Annual Weather Data (continued)

Month	Wind						Percent of possible sunshine	Average sky cover, tenths, sunrise to sunset	Number of days											Average station pressure mb
	Resultant		Average speed - km/hr	Fastest observed 1-minute value					Sunrise to sunset			Precipitation .025 cm or more	Snow, ice pellets 2.5 cm or more	Thunderstorms	Heavy fog, visibility 0.4 km or less	Temperature °C				
																Maximum		Minimum		
	Direction	Speed -km/hr		Speed - km/hr	Direction	Date			Clear	Partly cloudy	Cloudy					32° and above	0° and below	0° and below	-18° and below	Elev. 1620 meter
JAN	33	7.2	14.8	68	NW	22	58	5.7	11	6	14	6	1	0	2	0	3	26	0	836.4
FEB	33	5.1	13.7	51	NW	24	73	4.9	9	10	9	5	2	0	2	0	0	24	0	838.1
MAR	30	1.6	16.9	68	E	14	66	4.8	15	5	11	4	0	1	0	0	0	16	0	836.1
APR	27	3.1	17.1	58	N	30	70	4.5	13	9	8	3	0	1	1	0	0	6	0	835.1
MAY	22	2.3	15.8	58	E	23	68	5.3	9	13	9	11	1	5	0	0	0	0	0	836.1
JUN	14	3.7	15.6	61	E	23	79	3.4	17	8	5	6	0	5	0	19	0	0	0	839.8
JUL	09	3.7	14.6	61	E	15	79	4.2	14	11	6	5	0	4	0	27	0	0	0	840.2
AUG	14	5.1	14.0	76	SW	19	79	3.6	18	8	5	5	0	7	0	21	0	0	0	839.8
SEP	12	4.7	13.2	69	E	14	78	3.4	18	6	6	4	0	3	0	15	0	0	0	840.8
OCT	19	0.5	12.7	55	E	9	84	4.0	15	9	7	2	0	1	0	3	0	2	0	838.1
NOV	34	4.5	13.2	58	SW	4	75	3.6	16	9	5	4	0	0	0	0	0	23	0	839.1
DEC	02	3.2	11.4	56	E	26	80	3.8	17	7	7	4	1	0	0	0	0	30	0	841.5
YEAR	01	0.6	14.5	76	SW	AUG 19	74	4.3	172	101	92	59	5	27	5	85	3	127	0	838.4

Table 3. SCA—Indoor Environmental Conditions

Temperature
18 to 24 °C

Relative Humidity
40% - 60%

Interior Lighting
Fluorescent

Pressure
100 kPa (constant when all doors are closed)

Table 4. Secure Cargo Area—Research Data on Threat

Intelligence Sources

National government information:

- Materials were recently confiscated from a militia's hiding place, which was located more than 600 miles from the Hartley Hub. Included were a facility drawing of the Hartley Hub with circles drawn around the SCA and the airport terminal, various weapons including automatic weapons, some explosives, and evidence of correspondence and communication with a foreign terrorist group.
- Surveillance of several members of the militia shows frequent trips to the Hub.

Crime Study

An analysis of crime incidents leads to the following conclusions:

- A major bank robbery was carried out within the state two months ago. A group of four robbers escaped with a large amount of money. Investigations show the bank vault was entered by a tunnel which originated across the street from the bank.
- Nationally there have been many thefts of highly valuable objects. The crimes do not appear to be related. It is speculated that they were committed by several groups, possibly organized crime.

Professional Organizations

- A recent meeting of the SSI (Southwest Surety Institute) included a special session on analysis of threat to facilities and material. No substantiated data on threats were available. However, the general feeling among members was that cargo in shipment and staging are an attractive target.
- During a meeting of the Industrialists Society, concern was expressed by managers of corporations that some of their employees had been approached by unnamed groups to help them carry out theft of valuable equipment and materials from the corporations. The employees had been offered large amounts of money.

Literature Search

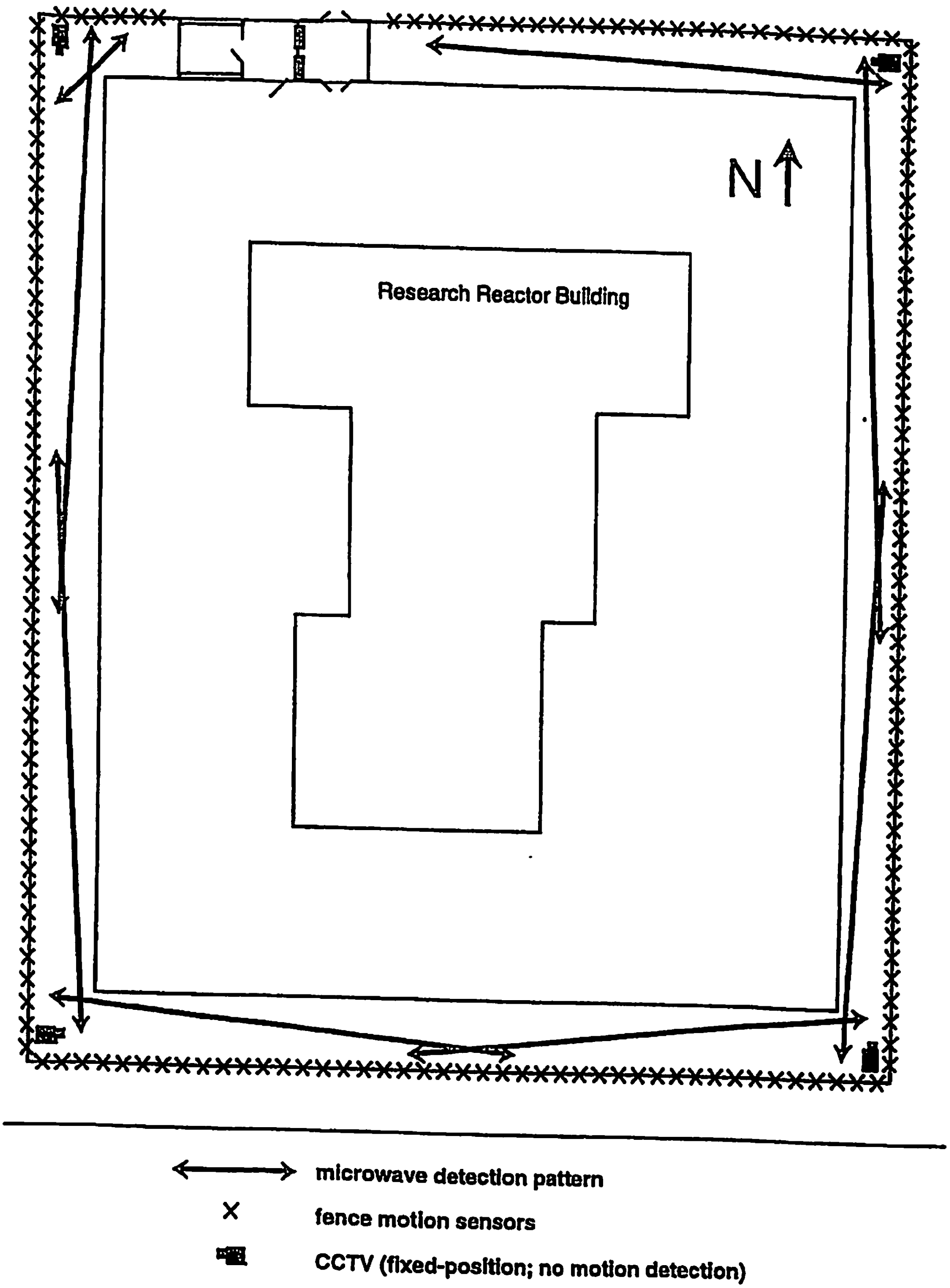
The literature search did not provide information about local or national threats to the SCA, but did provide information on international threats including:

- Plans (by a competitor) to steal critical assets of other companies.
- Threats made by a militia that they had the ability (skilled members and weapons including rocket propelled grenades) to take over or sabotage a cargo area using force. Investigations proved they did possess the weapons and equipment they claimed they had.
- A meeting of industrial groups was held to discuss various subjects including critical assets, safety against theft, and sabotage of critical assets during transportation and storage.

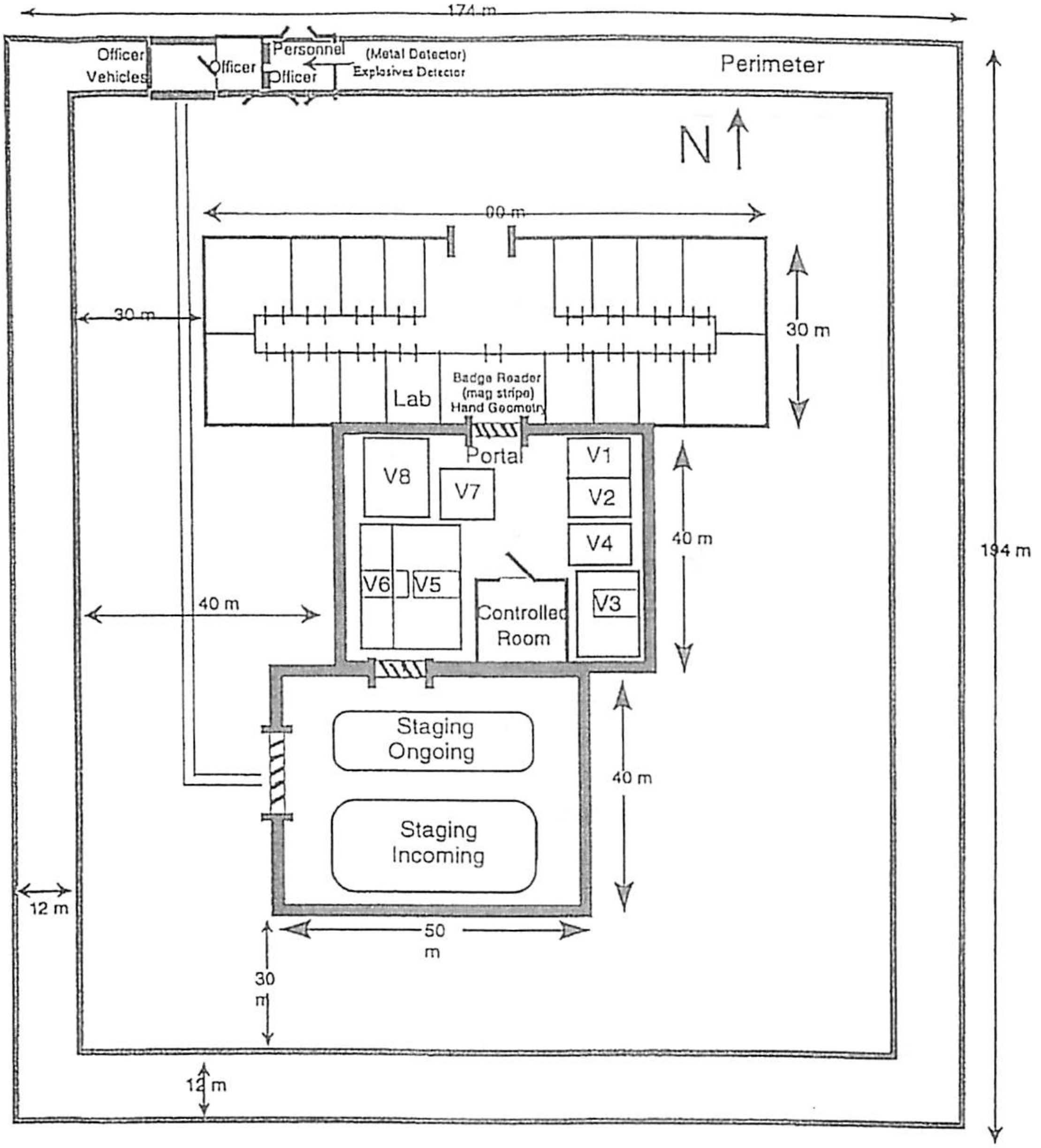
Site-Specific Data

- An analysis of the backgrounds of the employees of Hartley Hub and of the population of the community did not provide any information that would suggest a concern of threat to the SCA.
- There have been two serious disputes over labor issues at Hartley Hub in the past five years.
- Local news media publicize the SCA as the security system "that can't be beaten."
- All employees at the SCA submit to drug screening and a criminal background check, and personal references are checked before hiring.

Secure Cargo Area —Exterior Protection Plan

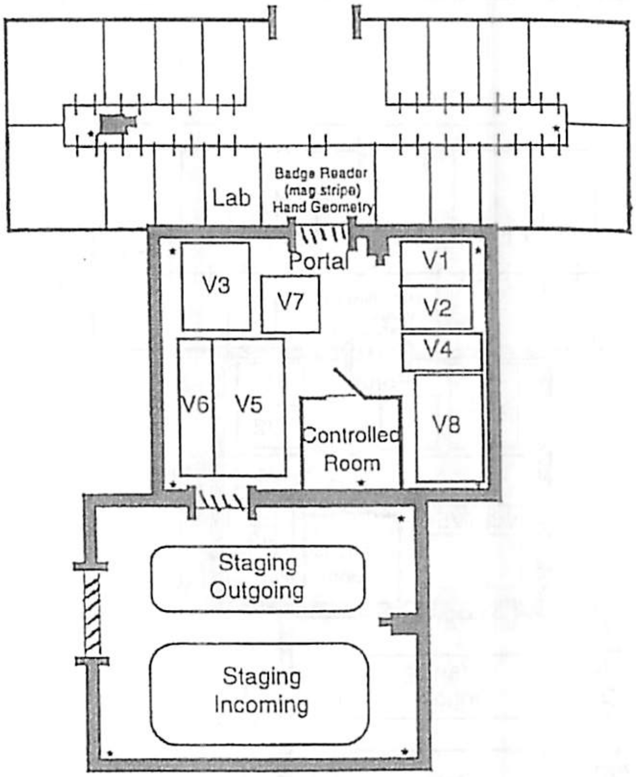

N
Research Reactor Building
⟷ microwave detection pattern
× fence motion sensors
▨ CCTV (fixed-position; no motion detection)

Secure Cargo Area—Wall Thickness and Distance



- ▬ 30 cm thick reinforced concrete
- ─ 15 cm thick reinforced concrete
- \\\\\\ 1.6 mm thick steel door (standard industrial grade) with balanced magnetic switch and embedded grid mesh
- □ 30 cm thick reinforced concrete plate (210 kg/cm No. 4 rebar) with vibration sensors
- ▤ 2-m chain-link mesh with outriggers (4-mm x 50-mm mesh)
- ▬ rolling gates
- ═ road

Secure Cargo Area—Interior Protection Plan



▬ 30 cm thick reinforced concrete

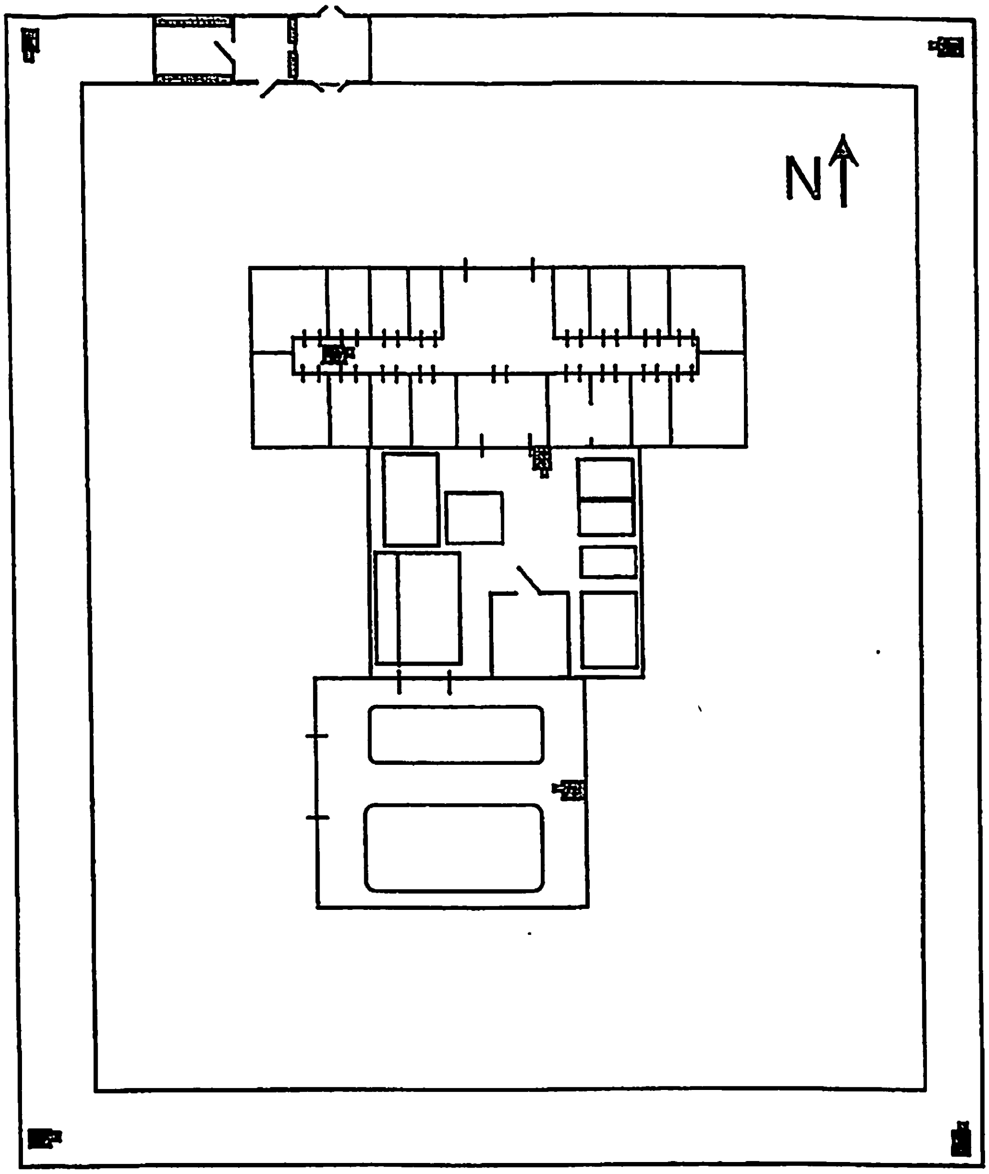
\\\\\\\\ 1.6 mm thick steel door (standard industrial grade) with balanced magnetic switch and embedded grid mesh

• microwave sensor

CCTV (fixed-position; no motion detection)

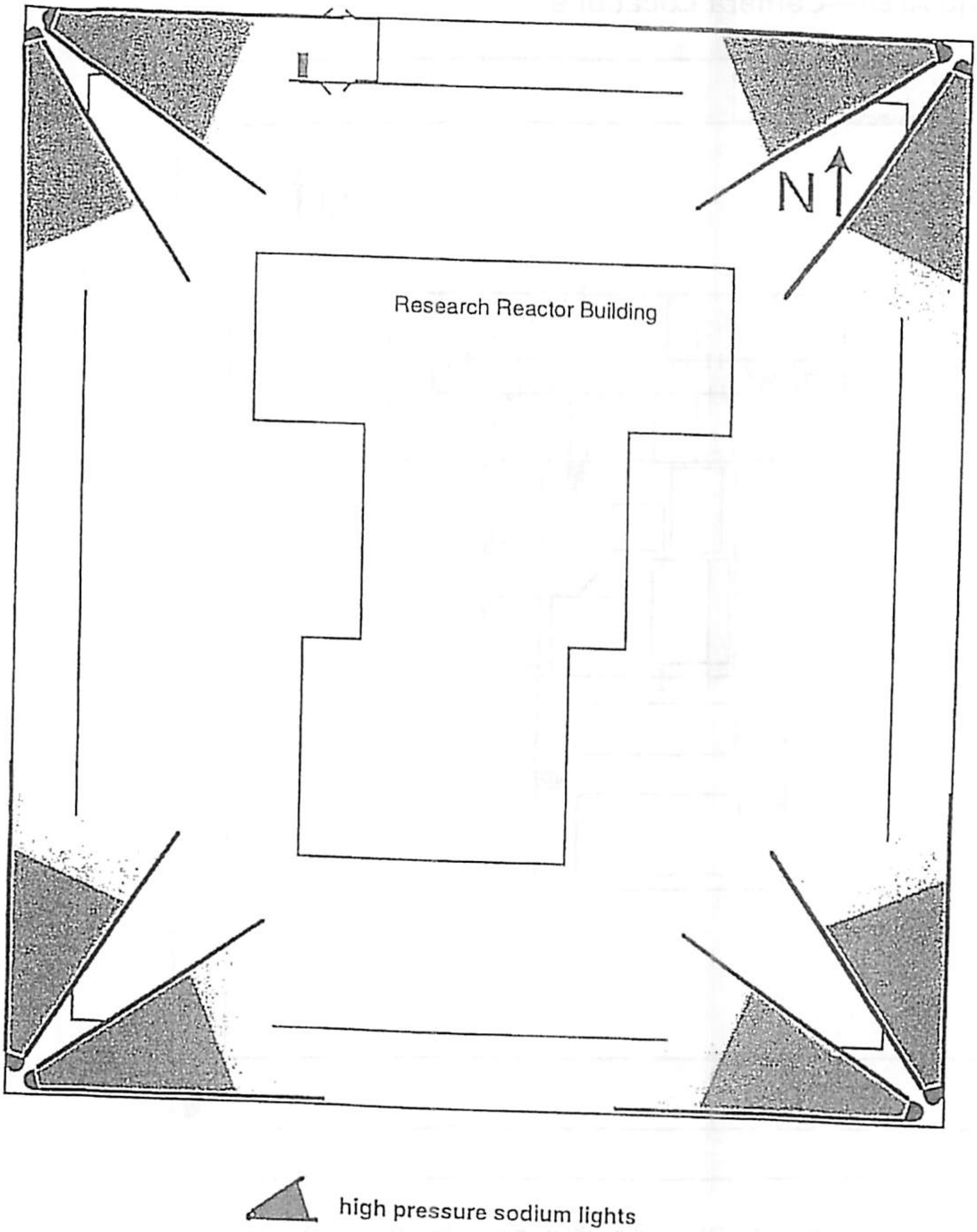
□ V1-8, storage vaults; material (sides and top) are hardened steel mesh

Secure Cargo Area—Camera Locations

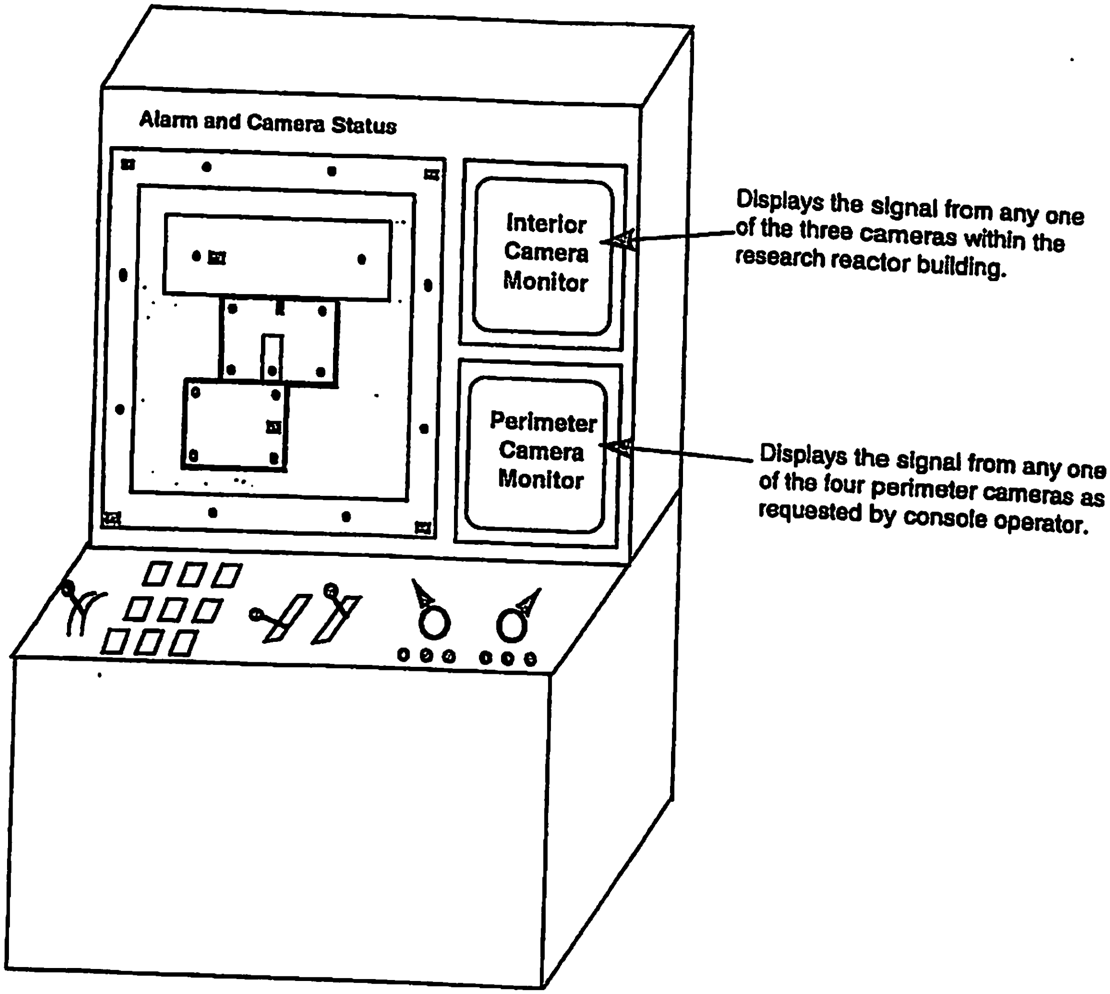


■ CCTV (fixed-position; no motion detection)

Secure Cargo Area—Lighting



Secure Cargo Area—Alarm and Camera Display Console



Displays the signal from any one of the three cameras within the research reactor building.

Displays the signal from any one of the four perimeter cameras as requested by console operator.

Camera selection is controlled from this console.

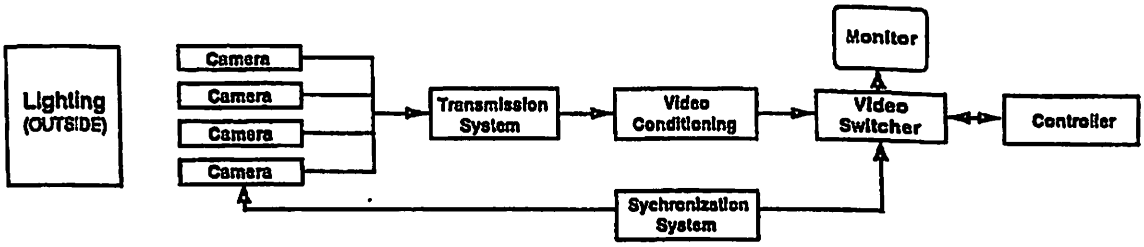
Panel light corresponding to the sensor or camera will light up when sensor is activated or camera is in use.

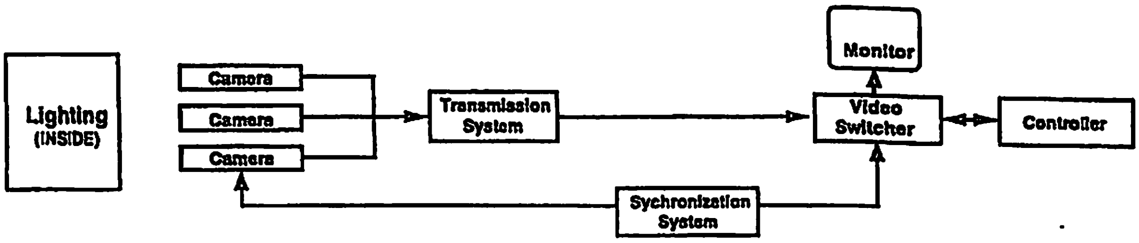
Audible tone is heard while sensor alarm is activated.

Operator can enter code to silence alarm.

Doors in the secure area cannot be remotely locked and unlocked for access control.

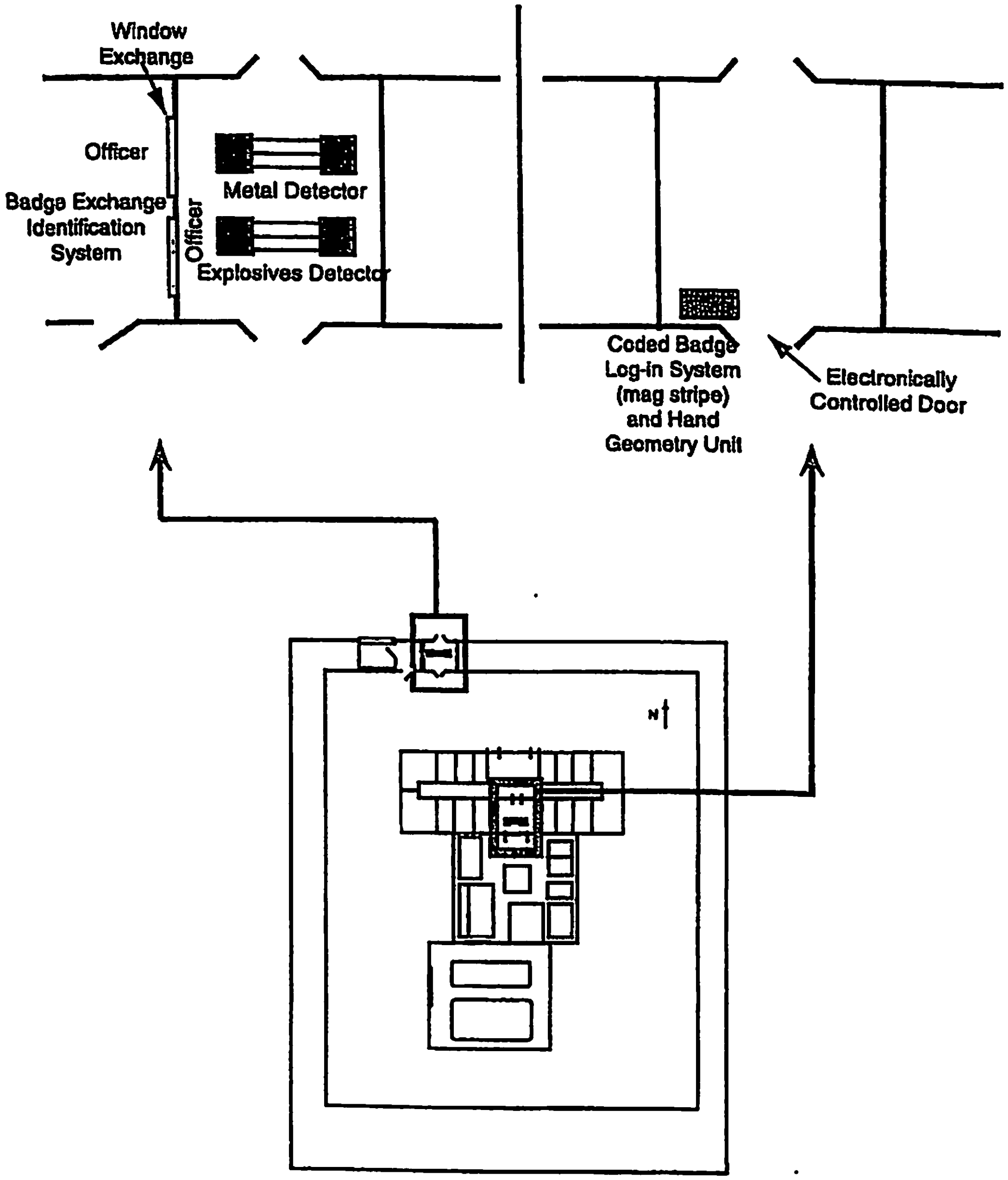
Video Monitoring System





- All cameras are fixed cameras - no pan/tilt/zoom capabilities.
- They do not have the ability to detect motion.
- There is no automatic alarm to video display system (when an alarm occurs, the operator must manually operate the controller)

Secure Cargo Area—Entry Control Plan


Window Exchange
Officer
Badge Exchange Identification System
Officer
Metal Detector
Explosives Detector
Coded Badge Log-in System (mag stripe) and Hand Geometry Unit
Electronically Controlled Door
N

Secure Cargo Area—Response Force Plan

Response Force	*Description*	*No. of Officers* *Workdays*	*Nights and Weekends*
R1	Airport Terminal Alarm Station	3	3
R2	Police Substation (Response Force Headquarters)	10*	10
R3	Secure Cargo Area	3	2
R4	Trucking Center	1	1
R5	Cargo Area	1	1
		18	17

*Includes site response team

Average Response Force Data

Average alarm communications time	= 0.1 minutes
Average alarm assessment time	= 0.5 minutes
Average response force communication time	= 0.3 minutes
Average response time (collecting equipment, and reviewing procedures)	= 20 minutes

Response Procedure for SCA Response Force

1. Alarm is detected at R3.
2. Local officer assesses alarm to determine if it is an intrusion or a false alarm.
3. Local officers report incident to R2.
4. Local officer communicates to other officers in affected areas to take immediate action.
5. R2 alerts response personnel to report to R2 for muster and deployment.
6. Response force at R2 collects firearms and protective gear.
7. Response team travels to position.
8. R2 officers deploy and proceed with interruption action, as necessary.

Secure Cargo Area—Communication Network

Communication Equipment

- Two or three officers at perimeter gate
- Three 6-watt hand-held radios
- Phone lines to headquarters
- 100-watt radio at the HQ

Communication Procedures

- Officers will carry a 6-watt radio with duress alarm.
- Officers will report all disturbances to the local alarm station for assessment.
- Each officer will be equipped with a microswitch, in gun holster, that will be monitored by a console operator at the protective force headquarters.
- If workers at SCA see something suspicious, they call front gate and the Lieutenant (console operator) decides what to do.

Part B EASI Model

Introduction

To look at EASI Examples click here

EASI is a simple calculation tool that quantitatively illustrates the effect of changing physical protection parameters along a specific path. It uses detection, delay, response, and communication values to compute the probability of interruption P_I. But, since EASI is a path-level model, it can only analyze one adversary path or scenario at time. Path level means that the model analyzes the protection system performance along only one possible adversary path or one adversary scenario. Even so, it can be used to perform sensitivity analyses and analyze PPS interactions and time trade-offs along that path.

For theft or sabotage attempts to be defeated, the response force must be notified of the attempt while sufficient time remains to respond and interrupt the adversary. Communication of the alarm to an operator and to the response force, therefore, is a factor in the analysis. An adversary interruption occurs in the EASI model if the PPS works properly, resulting in confronting the adversary with a response force large enough to prevent them from proceeding further along their path. The input for the model requires (1) detection and communication inputs as probabilities that the total function will be successful and (2) delay and response inputs as mean times and standard deviations for each element. The output will be the P_I, or the probability of intercepting the adversary before any theft or sabotage occurs. After obtaining the output, any part of the input data can be changed to determine the effect on the output. However, because EASI is a path-level model, as systems get larger and more complex, better computer models are needed to perform the analysis of multiple paths. This point will be discussed later in the chapter, in the section titled Adversary Sequence Diagrams (ASD). ASDs provide a graphical method to represent the protection elements in a system, which can serve as the interface between a human analyst and computer software.

The Input

In the EASI model, input parameters representing the physical protection functions of detection, delay, and response are required. Communication likelihood of the alarm signal is also required for the model. Detection and communication inputs are in the form of probabilities that each of these total functions will be performed successfully. Delay and response inputs are in the form of mean times and standard deviations for each element. All inputs refer to a specific adversary path.

The EASI input for the detection function is the P_D for each sensor encountered by an adversary. As discussed in the text, this probability is highly dependent on the capabilities of the adversary. The P_D is the product of the probability that the detector will sense abnormal or unauthorized activities by the adversary (P_S), the probability that an alarm indication will be transmitted to an evaluation or assessment point (P_T), and the probability of accurate assessment of the alarm (P_A). P_S was discussed in Chapter 5 and assessment was covered in Chapter 8. The relationship among these performance measures for P_D can be summarized as:

$P_D = P_S * P_T * P_A$

The communication of an alarm condition to the response force is input into EASI as the probability of guard communication, P_C. In most PPS, the likelihood of successful communication to the response force increases with time. The value entered into EASI for P_C is the probability of guard communication associated with the guard communication time included in the response force time (RFT). Evaluation of many systems designed and implemented by Sandia National Laboratories indicates that most systems operate with a P_C of at least 0.95. This number can be used as a working value during the analysis of a facility, unless there is reason to believe that this assumption is not valid. If actual testing at a facility yields a different P_C, this number should be used; if guard communication appears to be less dependable, a lower value can be substituted in the model. Factors that may influence P_C include lack of training in use of communication equipment, poor maintenance, dead spots in radio communication, or the stress experienced during an actual attack. This flexibility allows the analyst to vary P_C as needed to correctly represent this function.

The delay time required by an adversary to travel a given path to a target can be thought of as the sum of the times required to perform certain tasks or travel distinct path segments. For the sake of simplicity, both task times and travel times are referred to as adversary task times. In general, it is not possible to predict the exact time interval necessary for the adversary to perform these tasks or proceed across these path segments. This is due to the fact that the adversary (or the response force) will not always perform a task within exactly the same time. For example, the adversary may take more or less time to get through a door or the response force might have trouble starting a vehicle. Over a number of attempts, some variation in delay values will be observed. To allow for this expected variation in EASI, these time intervals are modeled as random variables possessing an average or mean value and a standard deviation. The length of each of these successive adversary task times is input into EASI as a mean time and a standard deviation. Standard deviation is discussed in more detail below.

Response time is modeled in EASI as the time between the generation of an alarm signal by a sensing device and the confrontation of the adversary by a response force adequate to halt the progress of the adversary along the path. This time consists of the successive time increments listed below and in Figure 14-1 in the book.

- alarm communication time
- time required for alarm assessment
- guard communication time
- time required for the guards to prepare, to gather arms, to start vehicles, etc.
- guard travel time
- time required for the guard force to muster and deploy

Response time input to EASI is in the form of a single mean time and standard deviation representing the sum of all the elements shown above. Alarm communication and assessment times are incorporated into RFT within the EASI model to simplify data entry and handling. The use of RFT should not be confused with P_C. RFT is a measure of the time it takes to receive, assess, and respond to an alarm; P_C is a measure of the likelihood that there will be successful communication to the response force to carry out the response.

There is one final note on data input to the EASI model. The time data entered into EASI may be in units of seconds or minutes, but not both. Given this constraint, delay and RFT should be in the same unit. If delay times are entered in seconds and RFT in minutes, the discrepancy will affect the accuracy of the output.

Standard Deviation

To use the EASI model as effectively as possible, some knowledge of the term standard deviation is required. Standard deviation is a measure of dispersion of a set of related data. Suppose the response time of the guard force at a facility is measured five times and gives the results shown in Table 14-1.

Trial Number	Response Force Time (minutes)	$(X_I\text{-}X_{avg})$
1	9	0
2	7	-2
3	10	1
4	11	2
5	8	-1

Table 14-1 Guard Response Time Trials. Multiple tests were conducted to measure response force time at a facility. X_{avg} is the average of the five trials and X_i is the individual trial result.

Using this data, the average response time is (9+7+10+11+8)/5 = 9 minutes. The standard deviation is a measure of the amount that a given data point is likely to deviate from the mean of all the data. Quantitatively this is calculated as:

$$s_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x_{avg})^2}{n-1}} = \sqrt{\frac{0+(-2)^2+(1)^2+(2)^2+(-1)^2}{(5-1)}} = 1.58$$

This is the sample standard deviation, based on n =5 observations. If we were to collect many observations on the response time, the sample standard deviation, s_n, would tend towards S, the standard deviation for the true distribution of response times. The sample standard deviation, s_n, should not be used in the EASI model. This is because five data points are not sufficient to justify this estimate of the population standard deviation. A better approach would be to collect response time data over several months and divide the data into groups of five. Then find s_n for each group using the equation above, and average these values to estimate S, the population standard deviation. This will take a minimum of 30 data points, and 6 values of s_n. This average s_n can then be used in EASI as the standard deviation. As an alternative, tests at Sandia have shown that the standard deviation of a time event can be conservatively estimated at 30% of the mean and, therefore, if there have not been enough tests to establish a statistically significant standard deviation, one can simply use 30% of the estimated mean. These assumptions are equally applicable to delay times, i.e., there is a standard deviation associated with each mean time and the standard deviation can be approximated by using the mean + or - 30%. Use of the standard deviation for RFT and delay times allows consideration of the fact that guards will not always respond in exactly the same time, and that adversaries may take more or less time to penetrate barriers.

If we were to make many measurements of the RFT, we would expect to find a Gaussian distribution of data points as shown in the curve in Figure 14-2 in the book. In a Gaussian (or normal) distribution, 68% of the values are found within the interval (X_{avg}-S) and (X_{avg}+S). In the above case, this means that we would expect the RFT to be between 7.42 and 10.58 minutes 68% of the time.

The Output

The output of the EASI model is an estimate of the probability that a sufficient number of response force personnel will interrupt the adversary at some point before the adversary completes acts of theft or sabotage. The output is the probability of interruption, P_I. If there is one sensor on the path, this probability is calculated as:

$P_I = P_C{}^*P_D$

Using the Model

To use EASI, the initial step is the selection of an adversary action sequence. The selection should be based on thorough knowledge of the facility and reasonable assumptions about the adversary. Next, select a physical path to the asset corresponding to the chosen sequence. Visualize the adversary tasks along that path, and determine the location of sensors. Then, obtain the required data: (1) the probabilities of detection and communication and (2) the mean and standard deviation of task times and response times. Finally, enter the data into the computer and obtain the results. The real value of the EASI model does not end there, however, because the analyst now has the opportunity to change the input data and see what effect this has on the output. A few examples will demonstrate these effects.

EASI Examples

Consider the example where the adversary intends to sabotage a target in a vital area as shown in Figure 14-3. The adversary intends to penetrate the fence, travel to the building, force open a door, travel to the vital area, force open another door, and set and detonate an explosive device on the critical asset. Detection and delay values are shown in Figure 14-4 and the RFT is 300 seconds.

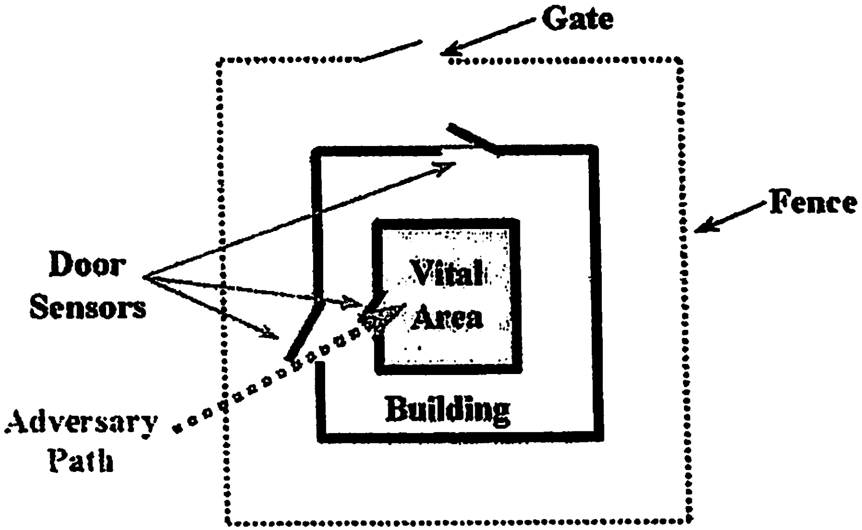
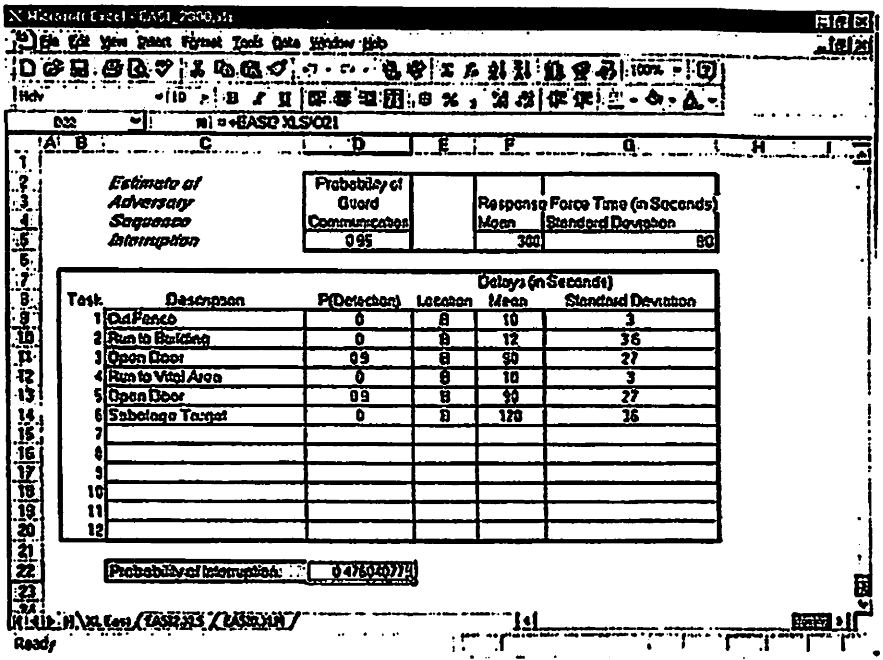


Figure 14-3 Adversary Path to Asset in a Vital Area. The adversary must cross the fence, approach the building, enter the outer door, travel to the asset location, enter an inner door, and then set-up the explosive charge at the asset.


Microsoft Excel - EASI_2000.xls
File Edit View Insert Format Tools Data Window Help
100%
Helv
10
=EASI2.XLS!C21
A B C D E F G H I
Ready

Estimate of Adversary Sequence Interruption

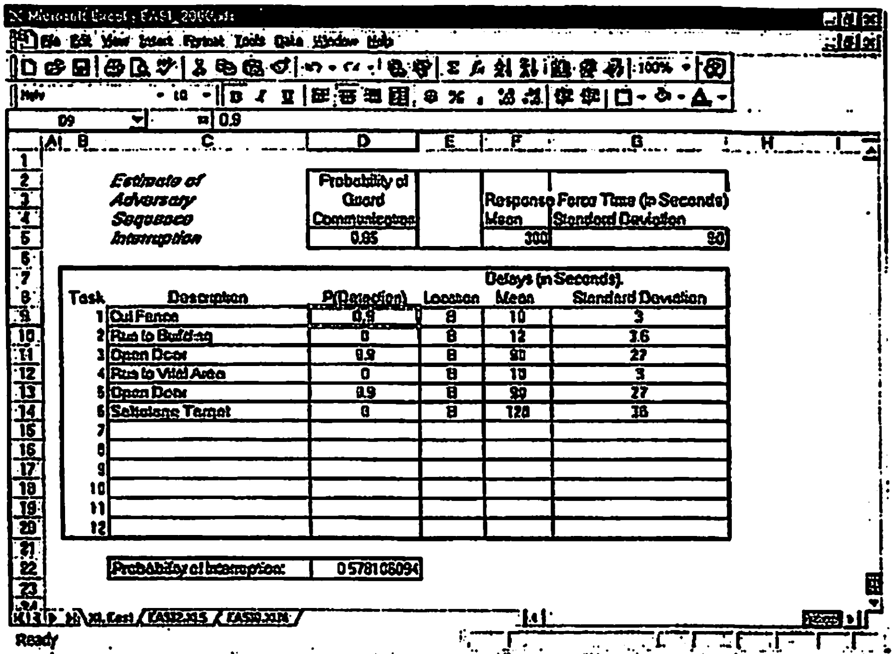
Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.95		300	90

				Delays (in Seconds)	
Task	Description	P(Detection)	Location	Mean	Standard Deviation
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption: 0.476040774

Figure 14-4 Results of EASI Analysis for Adversary Path. P_I is 0.48 for this path.

After entering this data in EASI, the result shows the probability of interruption is 0.48, as shown in Figure 14-4. The analyst may decide that this P_I is too low and that something should be done to improve this result. If a fence sensor with a probability of detection of 0.9 were added to the outer fence, the input would be as shown in Figure 14-5. The P_I in this upgraded case is 0.58, which may be satisfactory and may justify the installation of the fence sensor system.



Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds) Mean	Standard Deviation
1	Cut Fence	0.9	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.578106094

Microsoft Excel - EASI_2006.xls
File Edit View Insert Format Tools Data Window Help
100%
Helv
10
D9
= 0.9
A B C D E F G H I
XL East / EASI2.XLS / EASI3.XLS /
Ready

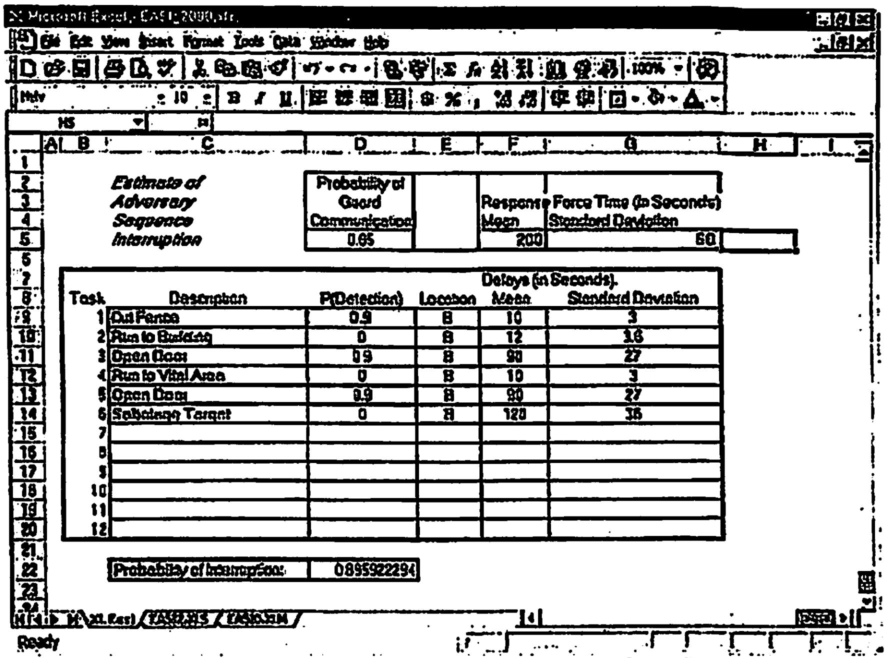
Figure 14-5 Results of EASI Analysis after Upgrade. A fence sensor with P_D of 0.9 was added to the outer fence resulting in an improved P_I of 0.58.

Exercise

The model is already open if you followed the download model instructions. Toggle between this page and the Excel EASI model using the Windows tool bar at the bottom of the screen to work the exercises along with the discussion below.

Task 1:

Replace P(Detection) from 0 to 0.9 (verify the result is .58 as shown above) If this value is still not acceptable, an additional upgrade could be modeled. For example, if the RFT is also reduced to 200 seconds, the new P_I is 0.90 (see Figure 14-6). This is a significant improvement and only required relocating guards closer to the target, i.e., low or no additional cost. Or, if preferred, guards could be left at their current location (RFT still 300 seconds) and delay can be doubled at the asset, perhaps by enclosing it in a hardened case. This would result in a P_I of 0.84 (see Figure 14-7). This is not quite as high as the previous upgrade, but might be easier or cheaper to implement or operationally be more acceptable. When the P_Is along all paths are approximately equal, the PPS is said to be balanced, i.e., all paths are equally difficult for the adversary to achieve their goal. Note that balance is achieved by mixing detection, delay and response components and that there are a number of possible combinations that will result in acceptable system performance. This provides the opportunity to select combinations that meet cost and operational requirements without compromising system effectiveness.



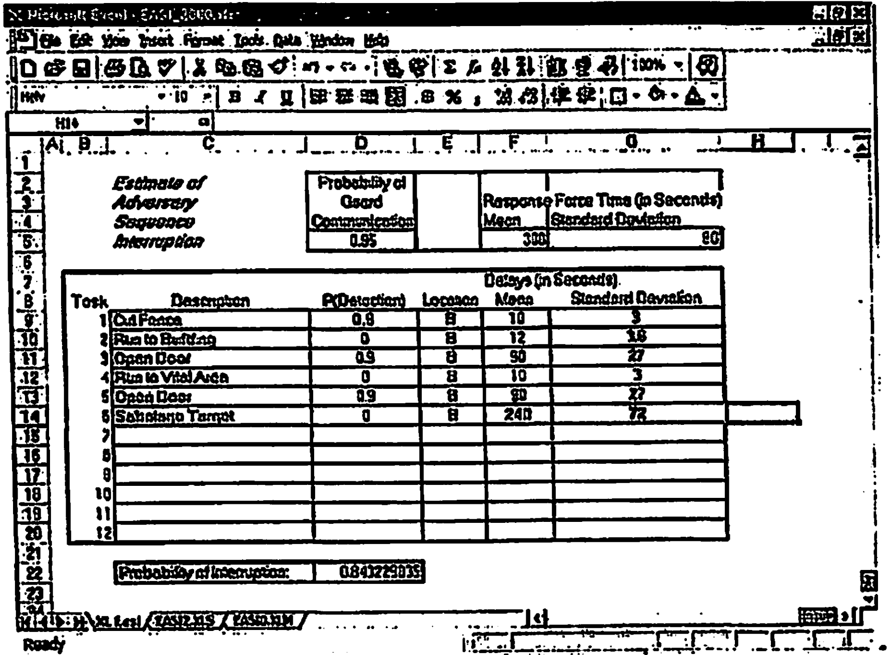
Estimate of Adversary Sequence Interruption

Probability of Guard Communication	Response Force Time (in Seconds) Mean	Standard Deviation
0.65	200	60

Task	Description	P(Detection)	Location	Delays (in Seconds) Mean	Standard Deviation
1	Cut Fence	0.9	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.895922294

Figure 14-6 EASI Analysis after Reduction in Response Force Time. Reduction of RFT and detection at the fence has increased P_I to 0.90.



Estimate of Adversary Sequence Interruption

Probability of Guard Communication	Response Force Time (in Seconds) Mean	Standard Deviation
0.95	300	90

Task	Description	P(Detection)	Location	Delays (in Seconds) Mean	Standard Deviation
1	Cut Fence	0.9	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	240	72
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.843229035

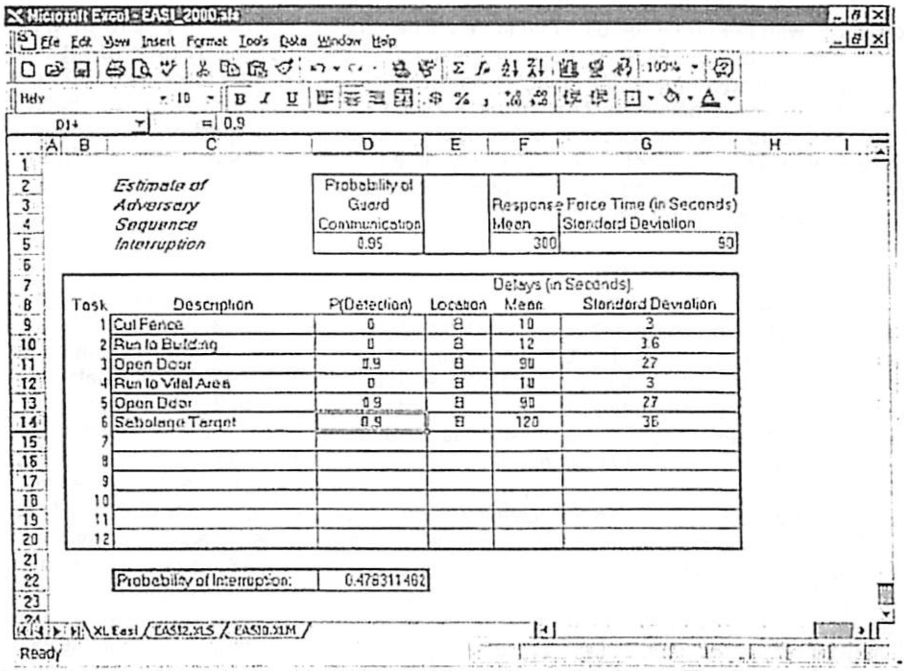
Figure 14-7 EASI Analysis after Addition of Delay at Asset. With detection at the fence and delay at the target, P_I is now 0.84.

These results demonstrate the utility of the EASI model, i.e., the ability to adjust protection elements and their performance in order to predict overall system effectiveness prior to implementation. Further manipulation of detection and delay components at different points on the path will emphasize the value of the security principles discussed throughout the text. These include detection early on the path and prior to delay, effectiveness of delay at the asset, the relationship among detection, delay and response functions, timely detection, and the principles of protection-in-depth and balanced protection.

Critical Detection Point

As described in Chapter 13 in the text, the critical detection point, or CDP, is the point on the path where the delay time remaining first exceeds the response force time. EASI cannot locate a CDP because the delay and response force times are random variables in a distribution, so there is a chance any point on the path will be the CDP during the actual attack. The concept of a CDP is too important to dismiss, however, because it gives valuable guidance on where to put additional protection, that is, add detection before or at the CDP and delay after.

Many of the more complex analysis tools, like SAVI or ASSESS, that find most-vulnerable paths use only the mean delay and response force times, because their algorithms fail when variation is introduced. Experience with these tools over the years has shown that effective systems can be designed by assigning the CDP based on the mean times, and then adding detection before this CDP and delay after it. This CDP, based on the mean values, will be what we refer to as the CDP in this chapter, rather than the more precise definition found in Chapter 13. For example, in Figure 14-4, the CDP is at the first door. To illustrate why this CDP is important for effective design, we will incorporate detection (P_D =0.9) at the target itself and show the results in Figure 14-8. The P_I is 0.48, which is the same as the baseline system. In Figure 14-9, 20 seconds of delay has been added at the fence, again resulting in a P_I of .48. Both of these upgrades were on the wrong side of the CDP and both had negligible effect on performance.



= 0.9

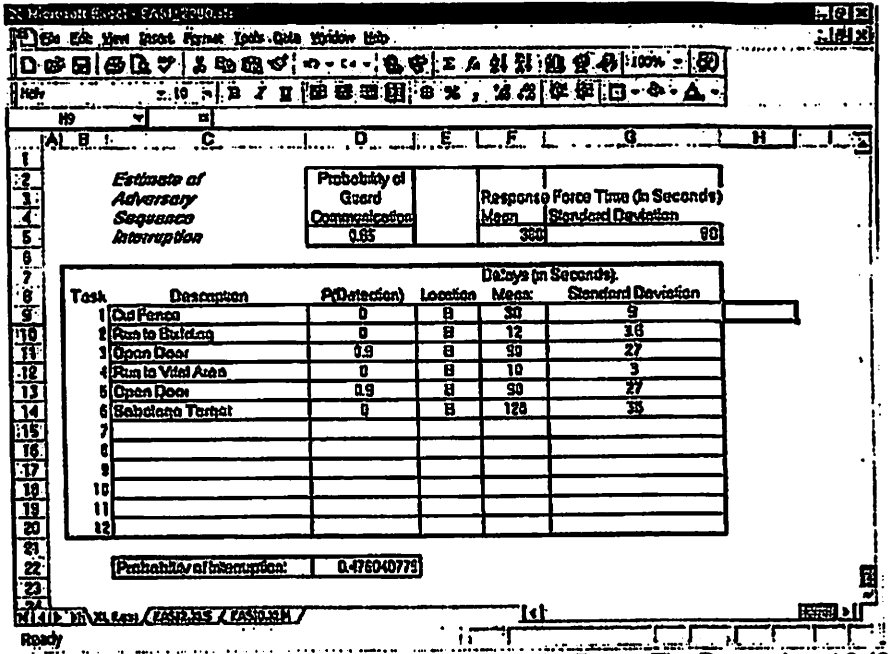
Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds) Mean	Standard Deviation
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0.9	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption: 0.476311462

Figure 14-8 EASI Analysis with Addition of Detection at the Asset. The P_I remains at 0.48.



Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
	0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Cut Fence	0	B	30	9
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	35
7					
8					
9					
10					
11					
12					

Probability of Interruption: 0.476040779

Figure 14-9 EASI Analysis with Addition of Delay at the Fence. The P_I remains at 0.48.

While it is practical to set the CDP based on mean delay and response force times, this must be done carefully, with the understanding that there will be variation in times. In Figure 14-4, the mean time remaining at the CDP exceeds the mean response force time by only 10 seconds--not a lot of leeway. Considering that the standard deviation for the response force time is 90 seconds, while that for the time remaining is 27 seconds, we see that 10 seconds leeway is probably insufficient to assure that any detection at this door will be effective. Typically, 30 seconds or more is desirable. This does not mean that a very large difference between RFT and time remaining on the path is by itself a design criterion, but it could become one if most of the detection is located on the path near the CDP.

Use of Location Variable in EASI

At this point, all but one of the required input elements to the EASI model have been discussed. This last input falls in the column labeled Location in the previous figures. Note that each of these results have a B in this column. The Location column is used to describe where in the model detection falls relative to delay for the specific protection element. Consider that if detection and delay both exist at an element, the detection may start before delay, at the end of delay, or somewhere in-between. Due to these possibilities, EASI allows assignment of detection relative to delay to more accurately model system effectiveness. To do this, entries are B for detection before delay, M for detection during delay (middle), and E for detection after, or at the end of, delay. Where there is no detection associated with the delay the location parameter will not matter. When the location is B, the delay time is calculated using the mean delay time for that element plus/minus the standard deviation; when an E is entered, EASI uses 0 as the time delay for this task. Use of an M indicates that the delay happens somewhere in between the before and end values, so is approximated as the one-half the mean plus/minus the standard deviation. The mathematical calculations for these assumptions are shown in Appendix B. Use of this location parameter allows the model to better allocate credit to the standard deviation of the delay time. This in turn allows the analyst to achieve a more realistic view of the probability of interruption by calculating the P_I based on the relationship of detection and delay time at each protection element. This is a complex point that may be best explained through the use of examples.

For example, a locked door with a balanced magnetic switch sensor might be assigned a location of E. This is because the sensor will not register an alarm until the door is opened a small distance. An attack on the door might be to pick the lock, then enter through the door. In this case, most of the delay came from the time to pick the lock, not to pass through the door, so the detection came at the end of the delay, which limits the effectiveness of the delay. An example of use of the M location parameter might be for the case where an adversary will use an explosive to penetrate a wall. In this case, the adversary must take time to set-up the explosive charge, then retreat to a safe distance during the detonation. At this point, the explosion would presumably be detected, but the adversary still has to return to the wall and get through the hole to continue the attack, so some delay still remains after detection. Use of the B parameter in the location column is exemplified by a volumetric sensor in a room monitoring a door. In this case, as soon as the adversary starts to penetrate the door, the sensor will detect the intrusion, and the adversary still must finish penetrating the door to get to the asset. The volumetric sensor detects before the door delay, so use of a B is appropriate.

Part C Questions: Design and Evaluation of Physical Protection Systems

1. Using Figure 14-4, add the following steps and performance measures that represent an adversary theft scenario, instead of sabotage. Assume RFT= 300 seconds and P_C= 0.95. What is the P_I? Where is the CDP, based on mean delays and RFT? What detection and delay improvements could be made?

Description	P_D	Location	Delay Mean	Standard Deviation
6. Remove asset	0.0	B	60	18
7. Exit Vital Area door	0.9	B	10	3
8. Run to 2nd outer door*	0.0	B	20	6
9. Exit outer door	0.9	B	0	0
10. Run to gate	0.0	B	15	4.5
11. Exit facility	0.2	B	12	3.6
*This not the same door that they entered through; it is the other door leading out of the building.				

Answer to Question 1

2. Using the initial theft scenario from question #4 above, assume the RFT is 600 seconds. What is the P_I? What if the RFT changed to 150 seconds?
Answer to Question 2

3. Using the sabotage scenario described in Figure 14-4, change the following locations and record the change in P_I. Explain your results. Be sure to change the location back to the initial value before making the next change.

a) Task 1, cut fence, change to M.
b) Task 6, sabotage target, change to E.
c) Task 3, open door, change to E.
d) Task 3, open door, change to M.
Answer to Question 3

4. Using the example from Figure 14-4, change the probability of communication to 0.8, 0.7, and 0.5. Record the new P_I for each of these values. Explain your results. What are some possible reasons for lowering the probability of communication in a PPS?
Answer to Question 4

Answers

Answer to Question 1:
$P_I = 0.46$
CDP is at Task 3, Open Door. This would explain why P_I didn't change much-detection and delay are not integrated together into an effective system.

Add detection at the fence of 0.9, P_I =.57 Add 60 seconds delay at other outer door (note that it isn't the same one they used to come in, had a crash bar on it, that's why it was 0). P_I =.76. Might be OK, but do one more. An obvious one is to add delay at the target, but this one was done previously, so encourage them to use something different. Add 50 seconds delay at vital area door, P_I =0.86. Not bad. Do as many as you want, decide what is acceptable.

Answer to Question 2:
RFT= 600 seconds, P_I = 0.05
RFT= 150 seconds, P_I =0.92

Answer to Question 3:
a) Task 1, cut fence, change to M. P_I =0.48 (no change). This is because there is no detection here. In this case, there is no relationship between detection and delay.

b) Task 6, sabotage target, change to E. P_I =0.48 (no change). Same as (a). We have maximized the value of delay at the target without detection. This should also reinforce the effectiveness of delay at the target and the lack of effectiveness of detection at the target for a sabotage scenario.

c) Task 3, open door, change to E. P_I =0.20. When the location is B, we have delay before detection, and the calculation uses the mean delay time ±standard deviation. The calculation is now changed to using 0 as the mean value ±standard deviation. This means we get less credit for delay, which means we have less of a chance of success.

d) Task 3, open door, change to M. P_I =0.33. The calculation is now made using the mean value as half the mean ±standard deviation, so we get more credit for the delay remaining after detection.

Answer to Question 4:
P_C= 0.8, P_I=0.40
P_C= 0.7, P_I=0.35
P_C= 0.5, P_I=0.25

The probability of communication could change due to transmission failure of the sensor signal (broken wire or intermittent connection), low/no battery power in response force radios (bad maintenance), guards not sure how to operate radio (bad training), if an adversary is jamming communications, or under the stress of a simulation exercise/attack, guards forgot how to operate radio features. The idea here is that a number of things can influence the probability of communication, ranging from equipment failure to bad training. It is important to consider this in the analysis of the system. If you are uncertain of how good your system communication is, test it to decide. If you know that under certain weather or operational conditions (such as lightning storms or non-operational hours), your communication system is less reliable, this may require lowering the P_C used.

For example, if a PPS used wireless (RF) transmission of alarm signals, bad weather or adversary interference could prevent adequate transmission of the alarm condition. This would justify using a lower value to recognize the uncertainty within the system.

Back to Top

Created by Ryan Bedoe
April 3, 2001
Disclaimer

Table 14S–1. Penetration Times—Fences

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
2-m chain-link mesh with outriggers	Ladder	5.0	0.1	0.2	0.3	0.04
4-mm x 50-mm mesh	Tarpaulin	2.0	0.1	0.2	0.3	0.04
	Pliers	1.0	1.0	2.0	3.0	0.41
	Manual boltcutters	3.0	0.5	1.0	1.5	0.20
	Circular saw	10.0	0.5	1.0	1.5	0.20
	Manual boltcutters, gloves (more cuts)	3.5	0.75	1.5	2.25	0.31
	Circular saw (more cuts)	11.0	0.75	1.5	2.25	0.31
	Gloves	0.5	0.1	0.2	0.3	0.04
Vinyl-coated 3-mm x 50-mm mesh	Manual Boltcutters	3.0	0.5	1.0	1.5	0.20
	Pliers	1.0	1.0	2.0	3.0	0.41
	Circular saw	11.0	0.75	1.5	2.25	0.31
2-m chain-link mesh without outriggers	Ladder	5.0	0.1	0.2	0.3	0.04
Vinyl coated, 1.8-mm x 40-mm mesh	No equipment	0.0	0.05	0.10	0.15	0.02
	Manual boltcutters	3.0	0.5	1.0	1.5	0.20
	Pliers	0.5	1.0	2.0	3.0	0.41.
	Vise grip pliers	0.5	0.30	0.60	0.90	0.12

Table 14S–2. Penetration Times—Gates

Barrier Description	Penetration Equipment	Equipment Weight (kg)	Penetration Time (Minutes)			
			Min.	Mean	Max.	Standard Deviation
Chain-link mesh pipe						
2.4-m x 4-m chain-link gate on metal pipe frame, chained and padlocked	Truck	1,500.0	0.05	0.1	0.15	0.02
	Pliers	1.0	1.0	2.0	3.0	0.41
Chain-link mesh pipe						
1.2-m x 2.4-m gate, 11-gauge x 5-cm mesh on 4.8-cm metal pipe frame, chained and padlocked	Sledgehammer	5.0	0.5	1.0	1.5	0.20
	1.8-m pry bar	10.0	1.0	2.0	3.0	0.41
	Boltcutters	3.0	0.75	1.5	2.25	0.31
	Hacksaw	0.2	1.0	2.0	3.0	0.41

Table 14S–3. Penetration Times—Walls

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
Concrete—10-cm Thick, Reinforced						
Concrete—210 kg/cm^2 one layer, 6.4-mm dia., 15-cm x 15-cm mesh	Sldegehammer, hand boltcutters	10	2.0	4.0	6.0	0.82
	Sledgehammer, cutting torch	30	2.5	5.0	7.5	1.02
	Circular saw, sledgehammer	5	4.3	8.6	12.9	1.76
	Rotohammer, chisel, punch, sledgehammer, hand boltcutters, generator	50	3.2	6.4	9.6	0.57
	Explosives (1.0), sledgehammer, manual boltcutters	20	1.4	2.8	3.2	0.37
	Explosives (3.0), hand boltcutters	10	1.0	2.0	3.0	0.41
	Explosives (5.0), hand boltcutters	7	0.9	1.8	2.7	0.37
	Explosives (10)	10	0.8	1.6	2.4	0.33
Concrete—210 kg/cm^2 one layer No. 5 rebar, 15-cm centers	Sledgehammer, hand hydraulic boltcutters	20	2.4	4.8	7.2	0.98
	Sledgehammer, cutting torch	30	2.0	4.0	6.0	0.82
	Rotohammer, chisel, hand hydraulic boltcutters, generator	50	3.9	7.8	11.7	1.59

Table 14S–3. Penetration Times—Walls (continued)

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
Concrete—15-cm Thick, Reinforced						
Concrete—210 kg/cm^2 one layer, No. 4 rebar, 20-cm centers	Sledgehammer, hand boltcutters	15	4.0	8.0	12.0	1.63
	Explosives (1.0), sledgehammer, hand boltcutters	14	1.5	3.0	4.5	0.61
	Explosives (3.0), hand boltcutters	5	1.15	2.3	3.45	0.47
	Explosives (5.0), hand boltcutter	7	1.0	2.0	3.0	0.41
Concrete—20-cm Thick, Reinforced						
Concrete—210 kg/cm^2 one layer No. 6 rebar, 15-cm centers	Rotohammer, drill, sledge, chisel, punch, cutting torch, generator	65	7.0	14.0	21.0	2.86
	Explosives (2.0), sledgehammer, hand hydraultic boltcutters	30	2.6	5.2	7.8	1.06
	Explosives (3.0), hand hydraulic boltcutters	20	1.5	3.0	4.5	0.61
	Explosives (5.0), hand hydraulic boltcutters	22	1.5	3.0	4.5	0.61
	Explosives (12)	12	1.2	2.4	3.6	0.49

Table 14S–3. Penetration Times—Walls (continued)

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
Concrete—30-cm Thick, Reinforced						
Concrete—210 kg/cm^2 one layer, No. 4 rebar, 15-cm centers	Explosives (5.0), hand boltcutters	8	1.3	2.6	3.9	0.53
	Explosives (7), hand boltcutters	9	1.4	2.8	4.2	0.57
	Explosives (12), hand boltcutters	14	1.5	3.0	4.5	0.61
	Explosives (16), hand boltcutters	18	1.5	3.0	4.5	0.61
Concrete—46-cm Thick, Reinforced						
Concrete—350 kg/cm^2 three layers No. 6 rebar, 15-cm centers	Explosives (16), hand-held power hydraulic boltcutters, generator	282	3.0	6.0	9.0	1.22
Concrete—350 kg/cm^2 two layers No. 4 rebar, 15-cm centers	Explosives (20), hand boltcutters	22	2.0	4.0	6.0	0.82
Concrete—60-cm Thick, Reinforced						
Concrete—350 kg/cm^2 four layers No. 6 rebar, 15-cm centers	Explosives (30), gas-powered hydraulic boltcutters	59	4.4	8.8	13.2	1.80

Table 14S–4. Penetration Times—Doors

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
Sheet Metal						
Standard industrial pedestrian door, 1.6-mm metal, panic hardware, cylinder lock, rim set, butt hinges with removable pins	Explosives (1.0)	1.0	0.75	1.5	2.25	0.31
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit	171.0	1.6	3.2	4.8	0.65
	Cordless drill	2.7	1.5	3.0	4.5	0.61
	Pry bar	7.0	0.1	0.2	0.3	0.04
	Fire ax	4.5	1.9	3.8	5.7	0.78
	Hammer, suction cups, punch, chisel	4.0	1.0	2.0	3.0	0.41
	Suction cups, sledge, cutting torch	25.0	0.5	1.0	1.5	0.20
	Explosives (.5)	2.5	1.0	2.0	3.0	0.41
	Lock picking tools	0.2	0.10	2.5	5.0	1.0
	Pipe wrench	1.0	0.2	0.4	0.6	0.08
	Explosives (2.0)	2.0	1.0	2.0	3.0	0.41
Standard industrial pedestrian door, hollow steel 1.6-mm narrow glass one side, louvers near bottom	Hammer	2.0	0.15	0.3	0.45	0.06
	Fire ax	4.5	0.80	1.6	2.40	0.33

Table 14S–4. Penetration Times—Doors (continued)

			Penetration Time (Minutes)			
Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Min.*	*Mean*	*Max.*	*Standard Deviation*
Sheet Metal						
Standard industrial pedestrian door, hollow steel, 1.3-mm half glass expanded metal 2.8-mm grill	Grappling hook, wire cable, truck	1,620.0	0.3	0.6	0.9	0.12
	Manual boltcutters	4.5	0.5	1.0	1.5	0.20
Standard industrial vehicle door, hollow steel panel, 1.6-mm	Explosives (0.5)	0.5	0.45	0.9	1.35	0.18
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit, water	385.0	0.80	1.6	2.40	0.33
	Sledgehammer, cutting torch, fire-resistant gloves, water	275.0	1.5	3.0	4.5	0.61
	Truck	2,025.0	0.3	0.6	0.9	0.12
	Pry bar, wooden plank	9.0	.75	1.5	2.25	0.31
	Fire ax	4.5	1.10	2.2	3.30	0.45
	Explosives (1.0)	1.0	.75	1.5	2.25	0.31
Standard industrial vehicle door, roll-up steel, corrugated 1.6-mm	Explosives (0.5)	0.5	.50	1.0	1.5	0.20
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit, water	385.0	1.0	2.0	3.0	0.41
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit	171.0	0.65	1.3	1.95	0.27

Table 14S–4. Penetration Times—Doors (continued)

Barrier Description	*Penetration Equipment (kg of explosives)*	*Equipment Weight (kg)*	*Penetration Time (Minutes)*			
			Min.	*Mean*	*Max.*	*Standard Deviation*
Sheet Metal						
	Truck	2,025.0	0.35	0.7	1.05	0.14
	Pry bar, wooden plank	9.0	1.0	2.0	3.0	0.41
	Fire ax	4.5	1.10	2.2	3.30	0.45
	Explosives (1.0)	1.0	.75	1.5	2.25	0.31
Steel Plate						
Magazine door, 6.4-mm steel plate, one padlock	Explosives, linear-shaped charge (0.5)	0.5	0.40	0.8	1.20	0.16
	Sledgehammer, cutting torch, fire-resistant gloves, water	248.0	2.0	4.0	6.0	0.82
	Circular saw	16.0	2.1	4.2	6.3	0.86
	Suction cups, sledgehammer, chisel	4.5	0.6	1.2	1.8	0.24
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit, water	385.0	1.25	2.5	3.75	0.51
Steel Plate/Void/Steel Plate						
Heavy door with two large-hinged hasps for padlocking, 19-mm steel, 10-cm air space, 1.3-mm	Explosives (4)	10.0	0.75	1.5	2.25	0.31
	Sledgehammer, cutting torch, oxy-lance, fire-resistant suit, water	385.0	3.1	6.2	9.3	1.27
	Sledgehammer, cutting torch, oxy-lance, fire-resistant gloves	165.0	0.3	0.6	0.9	0.12

Figure 14S–5. Cutting Rates for Reinforcement Bar Using 1-Meter Boltcutters

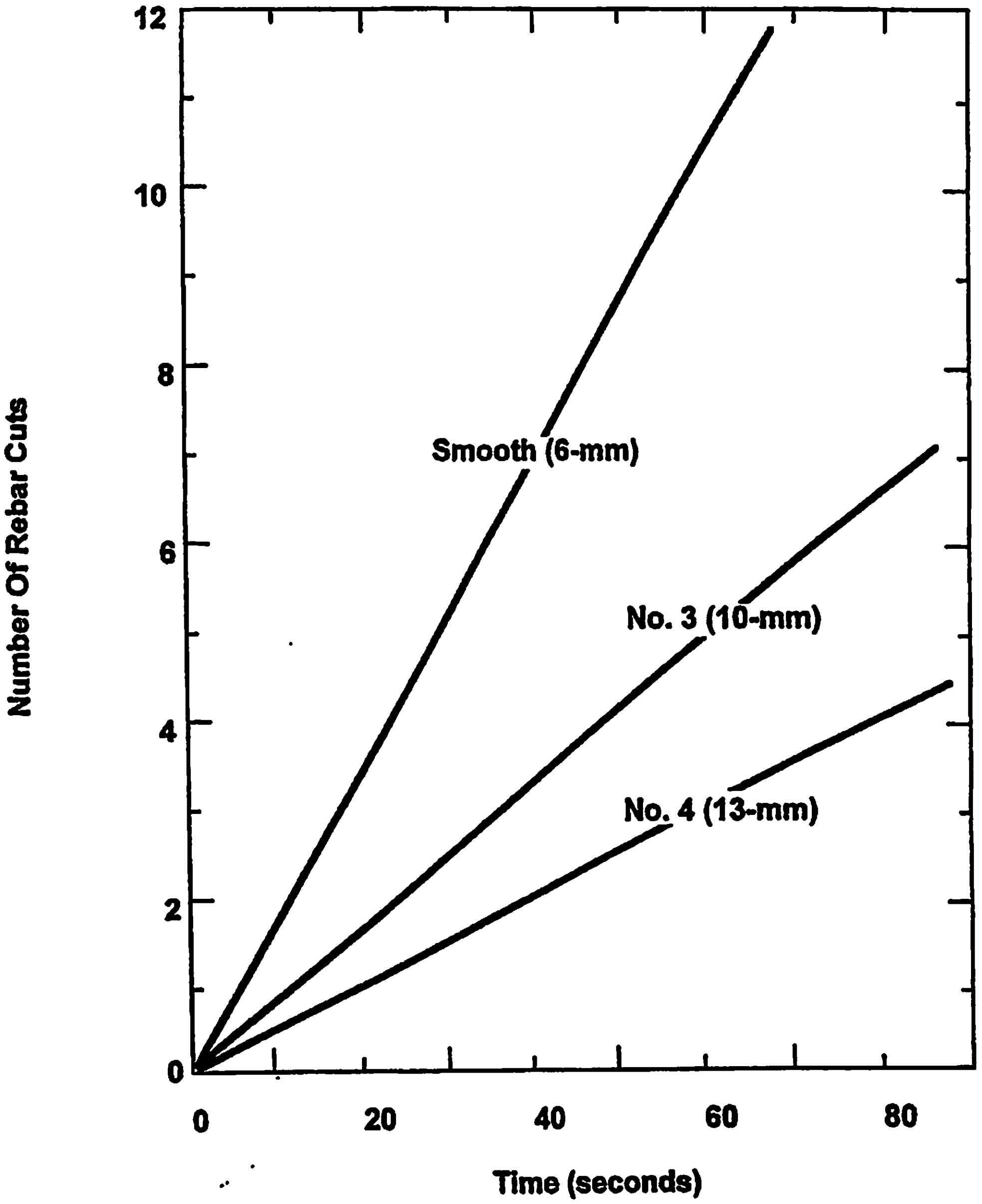


Figure 14S–6. Cutting Rates for Reinforcement Bar Using Portable Oxygen/Acetylene Cutting Torch

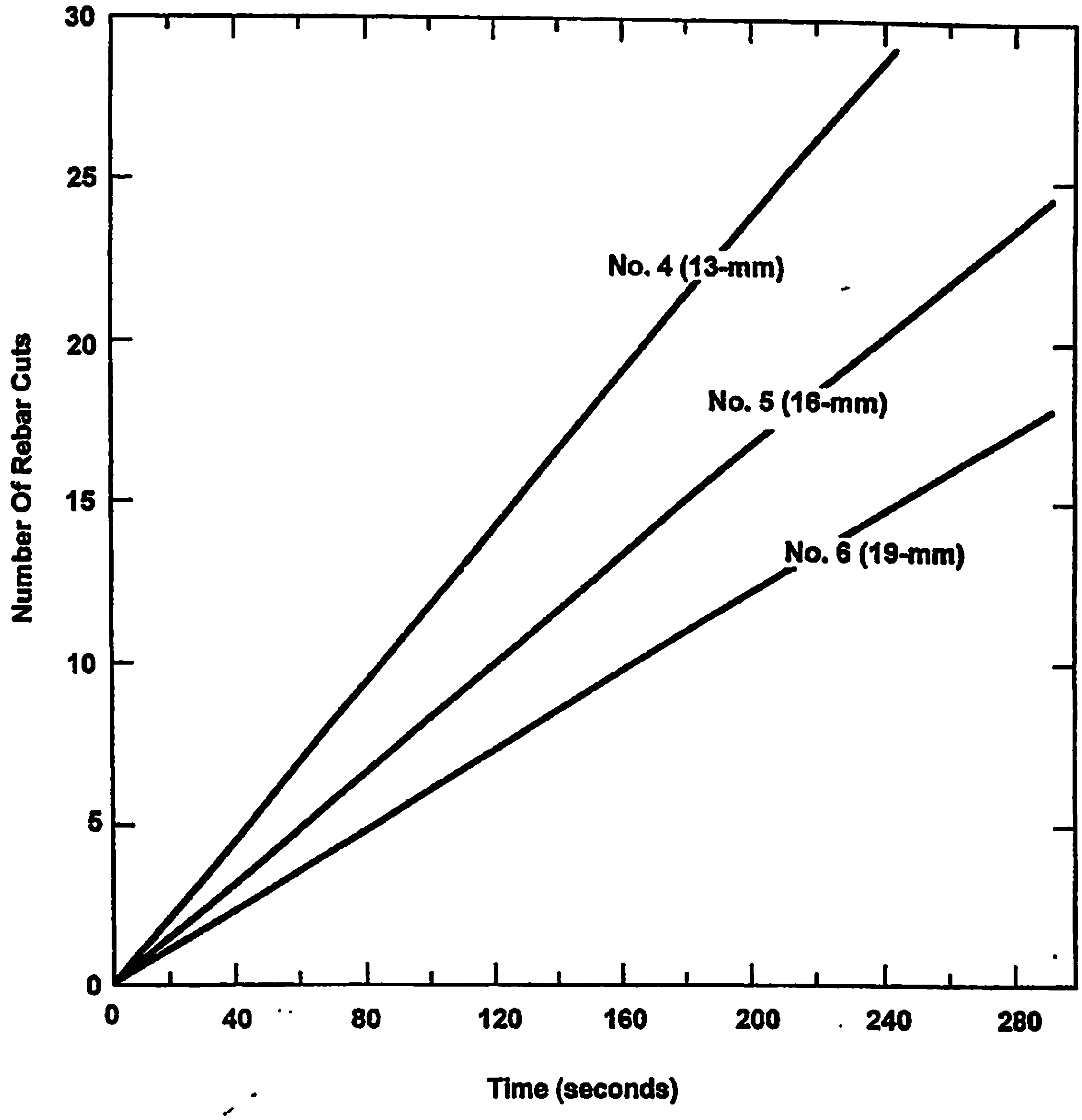


Figure 14S–7. Cutting Rates for Mild Steel Sheet & Plate Using Oxygen Acetylene Cutting Torch or Iron Oxygen Burn Bar

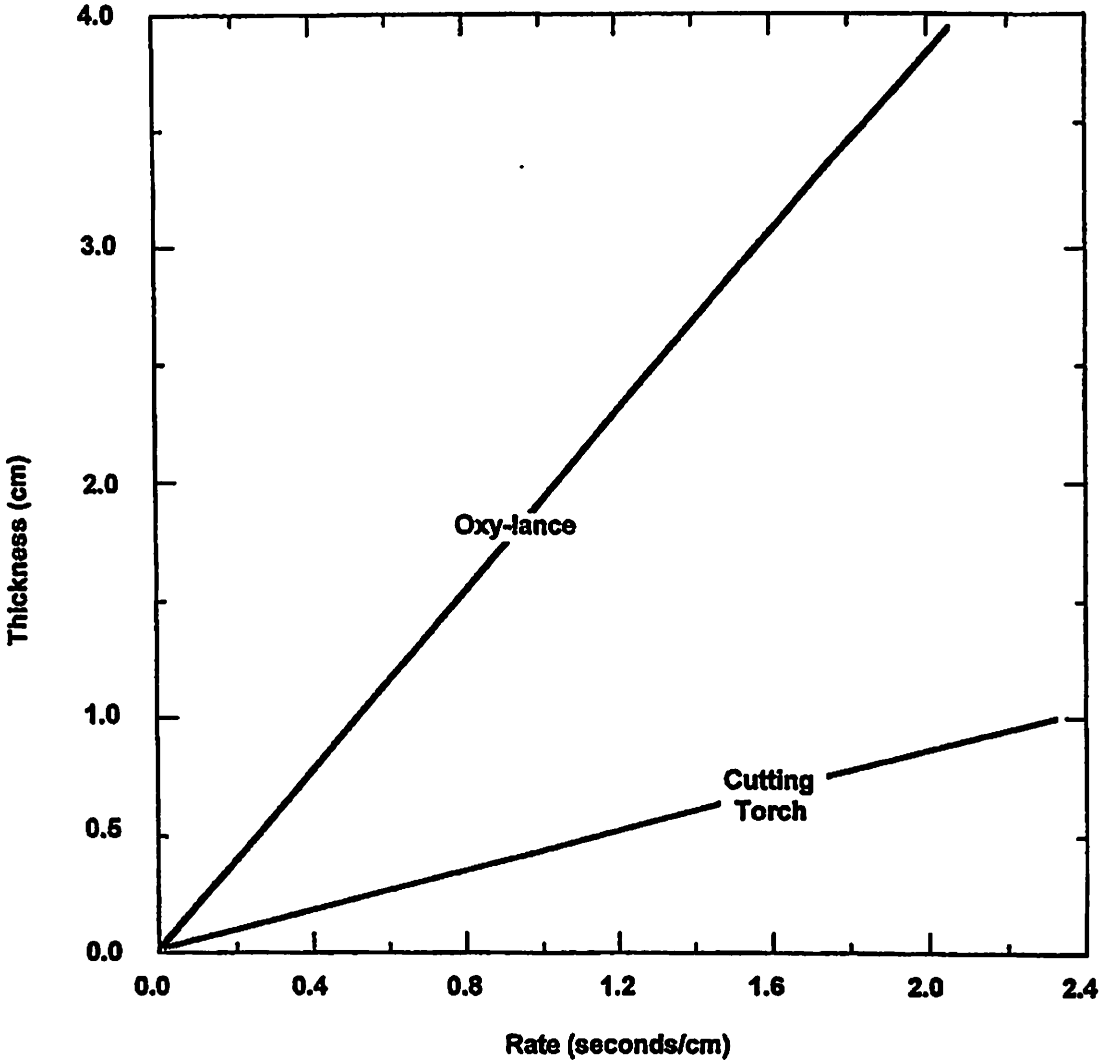


Figure 14S–8. Time Required to Set an Explosives Package as a Function of Package Weight

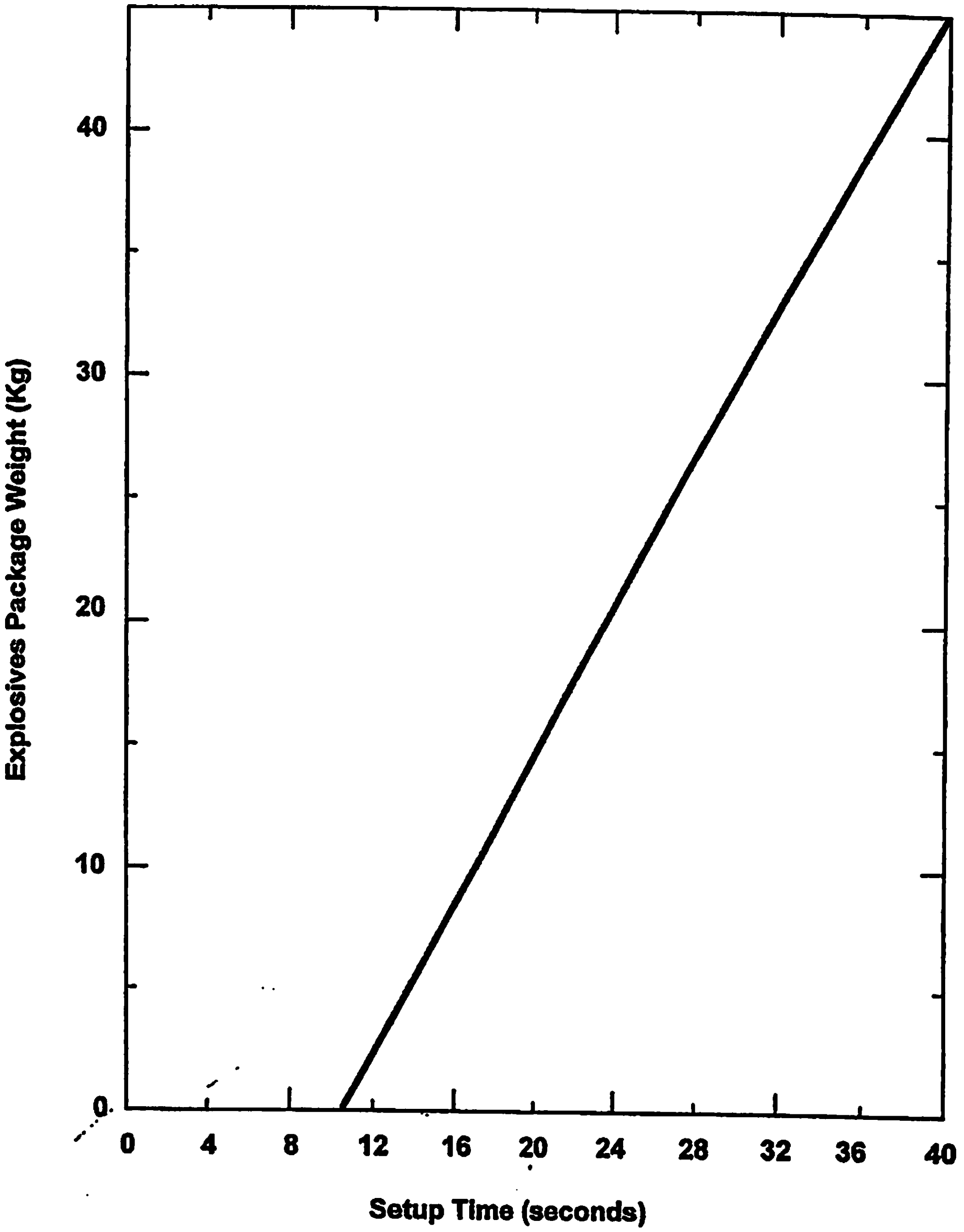


Figure 14S–9. Running Rates

1—On paved/unpaved ground
2—With tools (1.07-m boltcutters, pickax and shovel)
3—On sand
4—With weight (16 kg in toolbox)
5—With 2.4-m stepladder
6—With 10-m extension ladder (2 men)

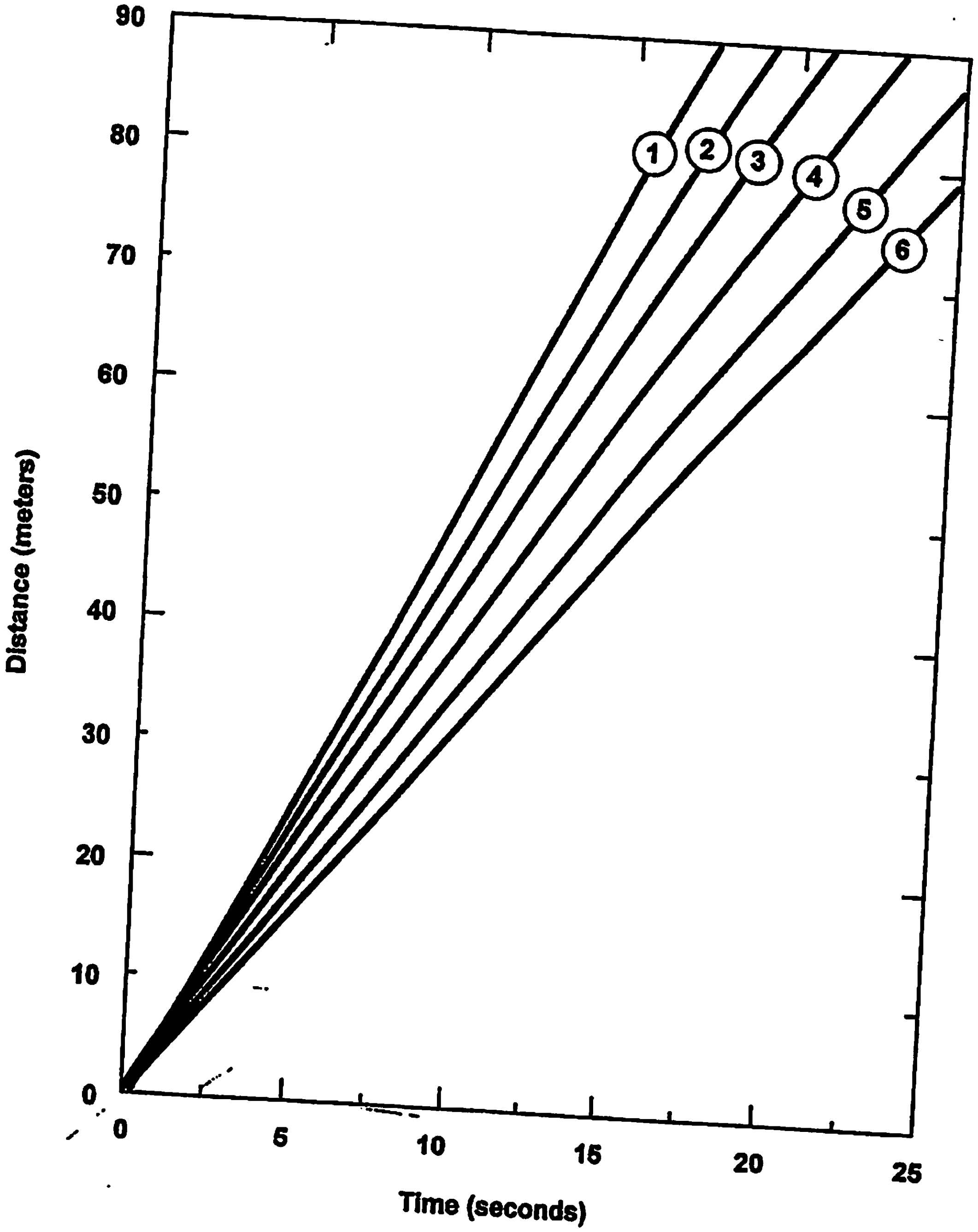
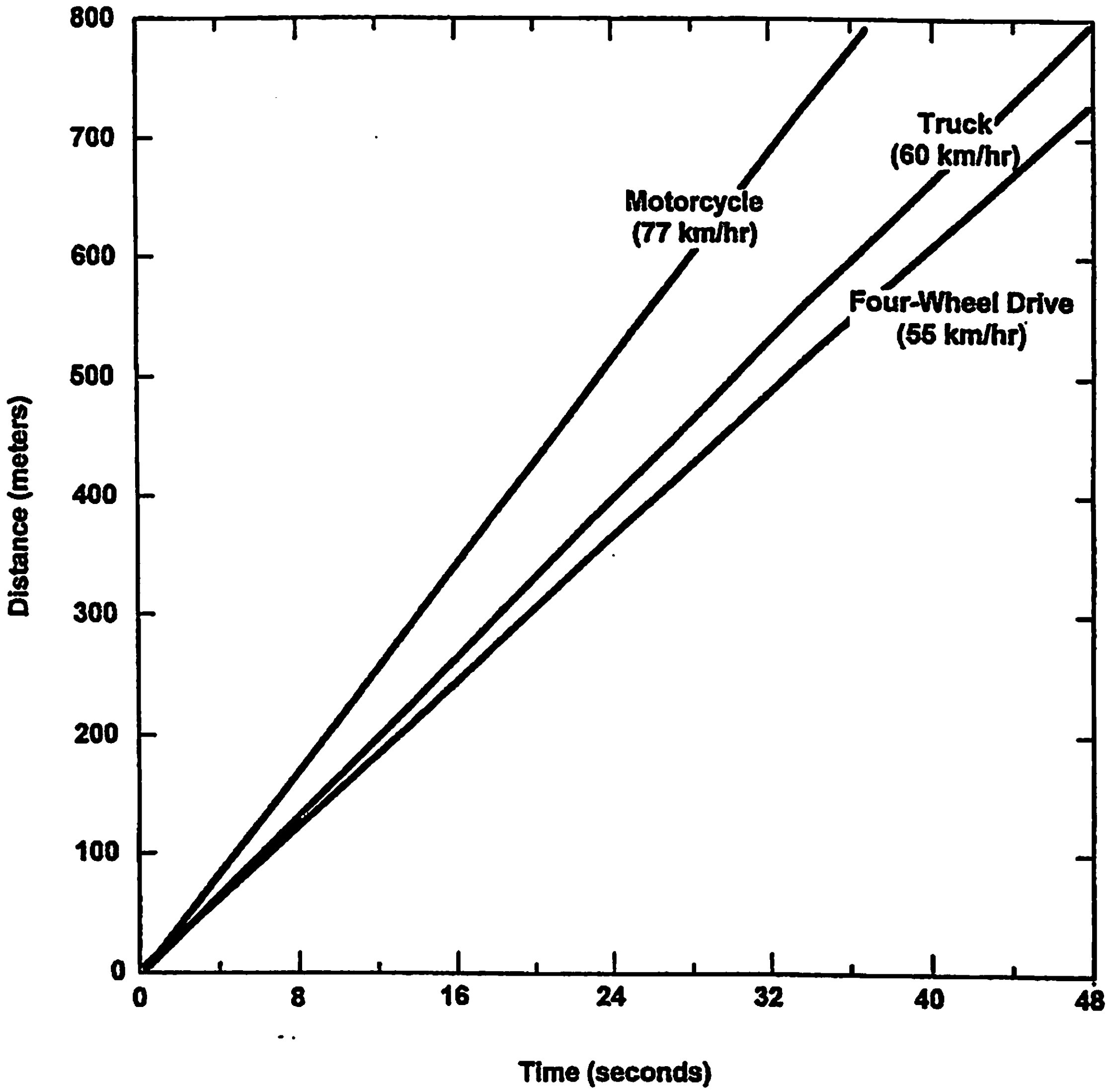


Figure 14S–10. Vehicle Rates for Experienced Drivers

TERRAIN— Road with one 90-degree turn.



VITA

DENNIS M. GIEVER

OFFICE:

Indiana University of Pennsylvania
Department of Criminology
Wilson Hall Room G-12
Indiana, PA 15705-1075
(724) 357-6941
E-Mail: dgiever@iup.edu

PERSONAL DATA:

Date of Birth: August 27, 1958
Married: Diane M. Giever
Children: Danielle (20 years)
Desirae (15 years)

EDUCATION:

Ph. D. Indiana University of Pennsylvania, Department of Criminology.
Dissertation: "An Empirical Assessment of the Core Elements of Gottfredson and Hirschi's General Theory of Crime."
Degree Awarded: December 1995.

M.C.J. New Mexico State University, Department of Criminal Justice.
Masters of Criminal Justice with a Graduate Minor in Experimental Statistics.
Thesis: "Predicting the Occurrence of Bank Robbery: An Environmental Approach."
Degree Awarded: 1992.

B.C.J. New Mexico State University, Department of Criminal Justice.
Bachelors of Criminal Justice.
Degree Awarded: 1990.

APPOINTMENTS AND AWARDS:

School of Graduate Studies and Research - Sponsored Programs Award for Outstanding Center, Institute, or Program - 2012.

School of Graduate Studies and Research - Sponsored Programs Award for Outstanding Achievement in Curriculum and Instruction - 2011.

The School of Graduate Studies and Research and the IUP Research Institute -

Outstanding Researcher - College of Health and Human Services, 2009.

Indiana University of Pennsylvania Office of Student Learning - Faculty/Staff Volunteer of the Year, 2008 - 2009.

The School of Graduate Studies and Research and the IUP Research Institute - Exploring Education Through Research - Dean's 2008-2009 Research Award.

School of Graduate Studies and Research - Sponsored Programs Award for Outstanding Achievement in Curriculum and Instruction - Information Assurance - 2005

Faculty Inductee of Phi Kappa Phi (National Honor Society) - 2003

Graduate Dean's Award for Outstanding Commitment to Sponsored Programs - presented to members of the Pine Grove Research Team - 2003.

El Paso Energy Foundation Faculty Achievement Award in Recognition of Outstanding University Teaching, New Mexico State University, 1997-1998.

Manuscript reviewer, Roxbury Publishing Company.

Manuscript reviewer, Journal of Research in Crime and Delinquency.

Manuscript reviewer, Criminology.

Manuscript reviewer, Justice Quarterly.

Manuscript reviewer, Crime and Justice Research.

Manuscript reviewer, Journal of Research in Crime and Delinquency.

Manuscript reviewer, Journal of Criminal Justice Education.

Manuscript reviewer, American Journal of Criminal Justice

Manuscript reviewer, The Prison Journal.

Manuscript reviewer, Security Journal

Manuscript reviewer, Journal of Crime & Justice.

Manuscript reviewer, Journal of Criminal Justice.

Manuscript reviewer, Criminology & Public Policy.

Manuscript reviewer, Criminal Justice Policy Review.

Manuscript reviewer, Journal of Drug Issues.

Manuscript reviewer, Person Custom Publishing.

Graduate faculty, Indiana University of Pennsylvania, 1998 - Present.

Graduate faculty, New Mexico State University, 1995 - 1998.

Outstanding Graduate Student Research Award, Indiana University of Pennsylvania, 1996.

Graduate Merit Scholarship, Indiana University of Pennsylvania, 1992 - 1993.

Alpha Phi Sigma (National Criminal Justice Honor Society) 1989 - Present.

Dean's Honor Roll (College of Arts and Sciences, New Mexico State University) 1989 -1990.

EMPLOYMENT:

2004 - present Professor of Criminology at Indiana University of Pennsylvania.

2008 - present Graduate Coordinator - FBI Programs.

1999 - 2008 Chairperson of the Department of Criminology at Indiana University of Pennsylvania. The duties of chair include: all scheduling of full time and temporary faculty courses, coordination of the criminology office, serving on numerous departmental, college and university committees as a representative for the department, coordination of department resources and budget, and general day to day operation of the department.

2001 - 2004 Associate Professor of Criminology at Indiana University of Pennsylvania.

1998 - 2001 Assistant Professor of Criminology at Indiana University of Pennsylvania. Courses taught: Quantitative Strategies for Analysis in Criminology (Graduate Level), System Dynamics in the Administration of Justice (Graduate Level), Advanced Applied Research (Graduate Level), Criminological Research Methods, and Law, Social Control, and Society. Responsibilities include advising students and serving on departmental and university committees.

1995 - 1998 Assistant Professor of Criminal Justice at New Mexico State University. Courses taught: Introduction to Criminal Justice, Introduction to Corrections, Introduction to the Nature of Crime, Research Methods, Hate Crimes, Introduction to Security Technology and Loss Prevention, Graduate Research Methods in Criminal Justice, Graduate Statistics in Criminal Justice, Graduate Policy Analysis and Program Evaluation, and Graduate Nature of Crime. Responsibilities included advising students and serving on Masters Committees.

1992 - 1995 Graduate Assistant assigned to the Center for Research in Criminology at Indiana University of Pennsylvania. Teaching Assistant in quantitative methods courses in criminology at masters and doctoral levels. Responsible for teaching the course sections on using SPSS (Windows & VAX Mainframe), conducting weekly review sessions, individual tutoring and consulting.

1991 - 1992 Instructor of Criminal Justice, New Mexico State University, Las Cruces, New Mexico. Courses taught: Introduction to Corrections (3 sections), and team taught Criminal Justice Planning and Crime Analysis (Computer lab portion of the class with Ron Pincomb). Instructed students in the use of DOS, Windows, Lotus, WordPerfect, dBASE as well as SAS, SPSS and E-Mail on the IBM Mainframe.

1990 - 1992 Graduate Assistant in the Masters Program at New Mexico State University.

1982 - 1988 General Manager of the Sally Port Inn Hotel, Roswell, New Mexico. Responsible for fiscal management, marketing, community relations and supervision of personnel.

PUBLICATIONS:

Avdija, A. S., & Giever, D. M. (2012). "The Impact of Prior Victimization and Socio-Economic Status on People's Crime-Reporting Behavior." *International Journal of Applied Psychology, 2*(4): 59-70.

Avdija, A. S., & Giever, D. M. (2011). "Path Analysis: Constructing a Causal Path Model of Correlates that Directly and Indirectly Affect Crime-Reporting Behavior." *Law Enforcement Executive Forum Journal,* 11(2): 95-122.

Myers, D. L., Lee, D., Giever, D. M. & Gilliam, J. (2011). "Practitioner Perceptions of Juvenile Transfer in Pennsylvania." *Youth Violence and Juvenile Justice, 9*(3): 222-240.

Avdija, A. S., & Giever, D. M. (2010). "The Influence of Citizen Interaction with the Police on Crime-Reporting Behavior: Its Manifestations Among University Students. *Journal of Criminology & Social Integration, 18*(2): 45 - 61.

Giever, D. M. & Hwang, EuiGab (2009). "Forensic Science Education and Training in the United States." *Journal of Korean Criminological Association, 3* (2): 173-190.

Winfree, L. T., Giever, D. M, Maupin, J. R. and Mays, G. L. (2007). "Drunk Driving and the Prediction of Analogous Behavior: A Longitudinal Test of Social Learning and Self-Control Theories." *Victims and Offenders,* 2(4): 327-349.

Giever, D. M. (2007). "Security Education - Past, Present and the Future." *Security Journal: Special Issue: 20th Anniversary, 20*(1), 23-25.

Giever, D. M. (2006). "Jails." In Joycelyn M. Pollock (Ed.) *Prisons Today and Tomorrow, Second Edition.* Boston, MA: Jones and Bartlett.

Gibbs, J. J., Giever, D., & Martin, R. (2006). "Integral Criminology and Criminal Justice." *AQAL: Journal of Integral Theory and Practice, 1*(1): 215-234.

Gibbs, J. J., Giever, D. M. & Higgins, G. E. (2003) "A Test of the Gottfredson and Hirschi's General Theory Using Structural Equation Modeling." *Criminal Justice and Behavior, 30*(4), 441-458.

Giever, D. M. (2003). "Jails." In J. Whitehead, J. Pollock & M. Braswell, (Eds.), *Corrections: Exploring Corrections in America* (pp. 109 - 153). Cincinnati, OH: Anderson.

Zimmerman, S., Gido, R., Myers, D., Giever, D., Dandeneau, C., Kiehl, K. & Komorosky, D. (2000) "Establishing a Research Institution: The Partnership Between IUP and the Pine Grove Prison For Violent Youthful Offenders." *Journal for Juvenile Justice and Detention Services, 15*(2), 67-84.

Winfree, L. T., Jr. & Giever, D. (2000). "On Classifying Driving-while-intoxicated Offenders: The Experiences of a citywide D.W.I. drug court." *Journal of Criminal Justice, 28*(1), 13-21.

Ruddell, R., Mays, G. L. & Giever, D. (2000). "Transferring Juveniles to Adult Courts: Recent Trends and Issues in Canada and the United States," in G. L. Mays and Peter R. Gregware (Eds.) *Courts & Justice: A Reader* (2nd ed.) (pp. 400-418). Prospect Heights, IL: Waveland.

Gibbs, J. J., Giever, D. M. & Pober, K. A. (2000). "Criminology and the Eye of the Spirit: An Introduction and Application of the Thought of Ken Wilber." *Journal of Contemporary Criminal Justice, 16*(1), 99-127.

Gibbs, J. J., Hanrahan, K. J. & Giever, D. (1999) "Framing and Measuring Fear of Crime for Decision Makers." *Justice Professional, 11*, 287-296.

Giever, D.M. (1999). *Instructor's Manual for Exploring Criminal Justice: An Introduction* by Don M. Gottfredson. Los Angeles, CA: Roxbury.

Becknell, C., Mays, G. L. & Giever, D. (1999) "Policy Restrictiveness and Police Pursuits." *Policing: An International Journal of Police Strategies and Management, 22*(1), 93-110.

Giever, D.M. (1999). *Student Study Guide for Exploring Criminal Justice: An Introduction* by Don M. Gottfredson. Los Angeles, CA: Roxbury.

Gibbs, J. J., Puzzanchera, C., Hanrahan, K. J. & Giever, D. (1998) "The Influence of Personal Safety and other Environmental Concerns on Sense of Control and Emotional Well Being." *Criminal Justice and Behavior, 25*(4), 403-425.

Ruddell, R., Mays, G. L. & Giever, D. (1998) "Transferring Juveniles to Adult Courts: Recent Trends and Issues in Canada and the United States." *Juvenile & Family Court Journal, 49*(3), 1-15.

McAuley, K., Giever, D. M. & Mays, G. L. (1998, Fall). "Law Enforcement Attitudes Toward Treatment Oriented Sanctions: DWI Drug Courts." *AABSS Perspectives Journal* [Online]. Available: http://www.aabss.org/journal1998/mcauley.htm [1998, Fall].

Giever, D.M. & Lynskey, D. (1998). *Instructor's Manual for Contemporary Corrections*, by G. Larry Mays and L. Thomas Winfree Jr. Belmont, CA: Wadsworth.

Lynskey, D. & Giever, D.M. (1998). *Student Study Guide for Contemporary Corrections*, by G. Larry Mays and L. Thomas Winfree Jr. Belmont, CA: Wadsworth.

Gibbs, J. J., Giever, D. M. & Martin, J. S. (1998). "Parental Management and Self-Control: An Empirical Test of Gottfredson and Hirschi's General Theory." *Journal of Research in Crime & Delinquency*, *35*(1), 40-70.

Alexander, G., & Giever, D. (1997, Fall). "A Security Technology Minor." *The Technology Interface* [Online]. Available: http://et.nmsu.edu/~etti/ [1997, November 4].

Giever, D. M. (1997). "Jails." In J. M. Pollock (Ed.), *Prisons: Today and Tomorrow* (pp. 414 - 465). Gaithersburg, MD: Aspen Publishers.

Gibbs, J. J. & Giever, D. M. (1995). "Self-Control and Its Manifestations Among University Students: An Empirical Test of Gottfredson and Hirschi's General Theory." *Justice Quarterly*, *12*(2), 231-255.

WORK CURRENTLY UNDER REVIEW:

WORK IN PROGRESS

PROFESSIONAL PRESENTATIONS AND PAPERS READ:

"A Summary Presentation of the Correctional Education Clearinghouse: Goals and Activities." Presentation to the Pennsylvania Department of Corrections, Mechanicsburg, PA, 2012 (with Dan Lee).

"Correctional Education Data Repository and Network. Presentation to the Performance Measures Committee at the Association of State Correctional Administrators annual meeting, Phoenix, AZ, 2012 (with Dan Lee).

"Practitioner Perceptions of Juvenile Prosecution in Pennsylvania." Paper presented at the annual meeting of The American Society of Criminology, Washington, DC, 2011 (with Dave Myers, Dan Lee and Jay Gilliam).

"Correctional Education Data Guidebook." Presentation made at the Correctional Education Association: 2011 Leadership Forum, Annapolis, MD, 2011 (with Dan Lee and Michelle Tolbert).

"Practitioner Perceptions of Juvenile Defense Representation in Pennsylvania." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Toronto, Canada, 2011 (with Dave Myers, Dan Lee and Jay Gilliam).

"An Assessment of Juvenile Case Processing Capabilities in Pennsylvania." Paper presented at the annual meeting of The American Society of Criminology, San Francisco, CA, 2010 (with Dave Myers, Dan Lee and Jay Gilliam).

"A National Census of Correctional Education Programming." Paper presented at the annual meeting of The American Society of Criminology, San Francisco, CA, 2010 (with Dan Lee).

"Data Analysis: Integration and Sharing." Presentation made at the Correctional Education Association: 2010 Leadership Forum, Annapolis, MD, 2010 (with Dan Lee).

"Practitioner Perceptions of Juvenile Transfer in Pennsylvania." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, San Diego, CA, 2010 (with Dave Myers, Dan Lee and Jay Gilliam).

"Evaluating Juvenile Prosecution and Defense Capacity Building Projects in Pennsylvania." Paper presented at the annual meeting of The American Society of Criminology, St. Louis, Missouri, 2008 (with Dave Myers, Dan Lee and Jay Gilliam).

"Practitioner Perceptions of Balanced and Restorative Justice (BARJ) in Pennsylvania." Paper presented at the annual meeting of The American Society of Criminology, St. Louis, Missouri, 2008 (with Dave Myers, Dan Lee and Jay Gilliam).

"Forensic Science Education and Training in the United States." Paper presented to the Asian Association of Police Studies International Conference in Seoul, South Korea, October 2007 (with Eui-Gab Hwang).

"Juvenile Justice in the United States." Lecture presented to members of the Ministry of Justice at the Gobong Information Communication Middle and High School, Seoul Juvenile Training School, Seoul, South Korea, October 2007.

"Drunk-Driving and the Prediction of Analogous Behavior: A Longitudinal Test of Social Learning and Self-Control Theories." Paper presented at the annual meeting of The American Society of Criminology, Toronto, Ontario, Canada, 2005 (with L. Thomas Winfree, James R. Maupin and G. Larry Mays).

"Measuring Outcomes for Correctional Education." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Las Vegas, NV, 2004 (with Nanci Wilson, Sherwood Zimmerman, Hilary Staples and John Lewis).

"Information Assurance - Looking Toward the Future." Panel presentation at the Government Information Technology Executive Council, Information Processing Interagency Conference in Orlando, FL, 2004.

"Risk Mitigation: Minimizing Threats to Personnel, Property & Profits." Presentation to the fourth annual Entrepreneur's Growth Conference in Pittsburgh, PA, 2002.

"National Correctional Education Center." Presentation at the Correctional Education Association Region I Conference, Bolton Landing, NY, 2002.

"National Correctional Education Center." Presentation at the 57th Annual International Conference of the Correctional Education Association in Portland, OR, 2002.

"Developing an Interdisciplinary Program in Cyber Security/Information Assurance in a Criminal Justice or Criminology Program." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Anaheim, CA, 2002.

"Computer Security and Information Assurance: Can Criminal Justice/Criminology and Computer Science Programs Unite to Address this Emerging Problem?" Roundtable moderated at the annual meeting of the Academy of Criminal Justice Sciences, Anaheim, CA, 2002 (with David Myers).

"Analyzing Qualitative Data with NUD*IST Software." Workshop presented at the annual meeting of the Academy of Criminal Justice Sciences, Washington, DC, 2001 (with Jamie Martin).

"Gottfredson and Hirschi's General Theory: Testing the Substantive Model Using Random Allocation Measurement Models." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, New Orleans, LA, 2000 (with John J. Gibbs and George Higgins).

"Establishing a Research Institution: The Partnership Between IUP and the Pine Grove Prison for Violent Youthful Offenders." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, New Orleans, LA, 2000 (with Sherwood Zimmerman, Rosemary Gido, David Myers, Dawna Komorosky, Claire Dandeneau and Kraig Kiehl).

"Gottfredson and Hirschi's General Theory: A Test Using Structural Equation Modeling." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Orlando, FL, 1999 (with John, J. Gibbs).

"Integrating Security Technology into the Criminal Justice Curriculum." Paper presented at the annual meeting of the American Association of Behavioral and Social Sciences, Las Vegas, NV, 1999 (with G. Larry Mays and James Breckenridge).

"Comparing DWI Offenders in a New Mexico Municipal Court: When is a Duck not a Duck?" Paper presented at the annual meeting of the Western Society of Criminology, Newport Beach, CA, 1998 (with L. Thomas Winfree, Jr.).

"Gottfredson and Hirschi's General Theory of Crime and Youth Gangs: An

Empirical Test on a Sample of Middle-school Students." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Albuquerque, NM, 1998 (with Dana Lynskey and Danette Monnet).

"Examining the Role of Support by Family and Friends in Treatment Effectiveness Within a DWI Drug Court." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Albuquerque, NM, 1998 (with Cindy Bejarano and G. Larry Mays).

"Law Enforcement Attitudes Toward Treatment Oriented Sanctions: DWI Drug Court." Paper presented at the annual meeting of the American Association of Behavioral and Social Sciences, Las Vegas, NV, 1998 (with Kelly McAuley and G. Larry Mays).

"Empirical Testing of Gottfredson and Hirschi's General Theory of Crime." Paper presented at the annual meeting of the American Society of Criminology, San Diego, CA, 1997.

"Crime and the Media: The Public's Perception of Crime." Paper presented at the annual meeting of the American Society of Criminology, San Diego, CA, 1997.

"Criminology and the Eye of the Spirit: An Introduction and Application of the Thought of Ken Wilber." Paper presented at the annual meeting of the American Society of Criminology, San Diego, CA, 1997 (with J. J. Gibbs).

"Transferring Juveniles to Adult Courts: Recent Trends and Issues in Canada and the United States." Paper presented at the annual meeting of the Western and Pacific Association of Criminal Justice Educators, Reno, NV, 1997 (with Rick Ruddell and G. Larry Mays).

"Treating the Persistent DWI Offender: Applying the Drug Court Concept to Drunk Drivers." Paper presented at the annual meeting of the Western Social Science Association, Albuquerque, NM, 1997 (with G. Larry Mays and L. Thomas Winfree, Jr.).

"A Minor in Security Technology." Paper presented at the Gulf Southwest Section of the American Society of Engineering Educators, Houston, TX, 1997 (with George Alexander).

"Emotional Intelligence and Criminal Behavior: A Conceptual Framework and Empirical Test." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Louisville, KY, 1997 (with J. J. Gibbs and C. Puzzanchera).

"Evaluating a Metropolitan Area Driving-While Intoxicated (DWI) Drug Court." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Louisville, KY, 1997 (with L. Thomas Winfree, Jr.).

"Designed Against Crime." Paper presented at the annual meeting of the Western Social Science Association, Reno, 1996 (with L. Thomas Winfree, Jr. and G.

Larry Mays).

"An Empirical Assessment of the Core Elements of Gottfredson and Hirschi's General Theory of Crime." Paper presented at the annual meeting of the American Society of Criminology, Boston, 1995.

"Fear of Crime and Sense of Control." Paper presented at the annual meeting of the American Society of Criminology, Boston, 1995 (with John J. Gibbs, Charles Puzzanchera and Kate Hanrahan).

"Content Analysis." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Boston, 1995.

"Parental Management and Self-Control: An Empirical Test of Gottfredson & Hirschi's General Theory." Paper presented at the annual meeting of the American Society of Criminology, Miami, 1994 (with John J. Gibbs and Jamie S. Kerr).

"Self-Control and Its Manifestations Among University Students: An Empirical Test of Gottfredson and Hirschi's General Theory." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Chicago, 1994 (with John J. Gibbs).

"Frances Alice Kellor." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Chicago, 1994.

"Crime Prevention and Bank Robbery: An Environmental Approach." Paper presented at the Western Social Science Association's 34th Annual Conference, Denver, Colorado, 1992.

"Predicting the Occurrence of Bank Robberies: A Test of Three Models." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Pittsburgh, Pennsylvania, 1992.

"Environmental Factors Associated With Bank Robberies." Paper presented at the Southwest Association of Criminal Justice Educators Annual Meeting, San Antonio, Texas, 1991.

"Child Abuse: A Problem With Perception." Paper presented at the annual meeting of the Academy of Criminal Justice Sciences, Nashville, Tennessee, 1991 (with Joan Crowley).

REPORTS:

Final report to ARIN Regional Educational Service Agency on Project TIPS (1994) (with Bill Collins, Kate Hanrahan and Jamie Kerr).

FUNDED RESEARCH:

An Evaluation of Pennsylvania's Juvenile Prosecution and Defense Capacity Building Projects. Pennsylvania Commission on Crime and Delinquency, 2005-

2007 (with David Myers, Dan Lee and Jay Gilliam). $117,660.00

MS Program in Security Engineering Technology. Sloan Foundation/ Council of Graduate Schools, 2002 (with Mary Lynn Garcia).

Attack, Defend, Convict: An Interdisciplinary Program in Information Assurance. National Science Foundation, 2001 (with Bill Oblitey and Mary Micco). $250,764.00

University Senate Research Committee Award, Indiana University of Pennsylvania. "The Influence of Emotional Intelligence on Deviance Using Structural Equation Modeling," 2001 (with John J. Gibbs).

Development of a Security Technology Program, Department of Justice, 1997 (with Jeff Beasley). $2,000,000.00

Evaluating a Metropolitan - Area Driving-While-Intoxicated (DWI) Drug Court, National Institute of Justice, 1996 (with L. Thomas Winfree, G. Larry Mays, and Peter Gregware). $130,000.00

National Evaluation of G.R.E.A.T., National Institute of Justice, 1996 (with Finn-Aage Esbensen and others).

Senate Research Committee Award, Indiana University of Pennsylvania. "Empirical Test of General Theory of Crime," 1994 (with John J. Gibbs).

DEPARTMENT AND UNIVERSITY ADMINISTRATIVE ACTIVITIES:

Graduate Coordinator - FBI Programs, 2008 - Present.

Academic Computing Policy Advisory Committee - Co-Chair, 2006 - 2008, Member 2003 - Present.

Middle States Steering Committee, 2003 - 2006.

University Planning Council, Indiana University of Pennsylvania, 2002 - 2006.

Academic Council, Indiana University of Pennsylvania, 2002 - 2006.

College of Humanities and Social Sciences Technology Committee, Indiana University of Pennsylvania, 1999 - 2004.

College of Humanities and Social Sciences Honors Committee, Indiana University of Pennsylvania, 2000 - 2004.

Institutional Review Board (IRB), Indiana University of Pennsylvania, 1999 - 2006.

Methods Doctoral Qualifying Committee, Indiana University of Pennsylvania, 1998 - 1999, 2001 - 2002, 2007 - 2008.

Theory Doctoral Qualifying Committee, Indiana University of Pennsylvania, 1998 - 2000. 2002 - 2007.

Educational Services Funds Planning Committee, Indiana University of Pennsylvania, 1999 - 2008, (Chair). Responsible for developing a budget to disperse educational funds allocated to the Department of Criminology.

Advisory Committee of Distance Education, New Mexico State University, 1997 - 1998. Served as representative for the College of Arts and Sciences.

Enrollment Management Committee, New Mexico State University, 1996. Responsible for making a recommendation to the department and college in developing an enrollment cap for the Department of Criminal Justice.

Library Allocation Committee, Indiana University of Pennsylvania, 1994. Served as Chairperson. Responsible for the allocation of library purchase funds for the doctoral and undergraduate programs in the Department of Criminology.

Educational Services Funds Planning Committee, Indiana University of Pennsylvania, 1992. Responsible for developing a budget to disperse educational funds allocated to the Department of Criminology.

Criminal Justice Graduate Students Association, New Mexico State University, 1991 - 1992. Served as president. Responsible for general organization, dispersion of information, budgeting and allocation of travel funds.

Graduate Students Organization, New Mexico State University, 1991-1992. Served as representative of the Department of Criminal Justice.

PROFESSIONAL MEMBERSHIPS:

Academy of Criminal Justice Sciences

American Society of Criminology

ASIS International

The Mathematical Association of America

THESIS AND DISSERTATION ADVISEMENT

Doctoral Dissertation
Major Advisor 7
Committee Member 18

Master's Thesis
Major Advisor 8
Committee Member 10