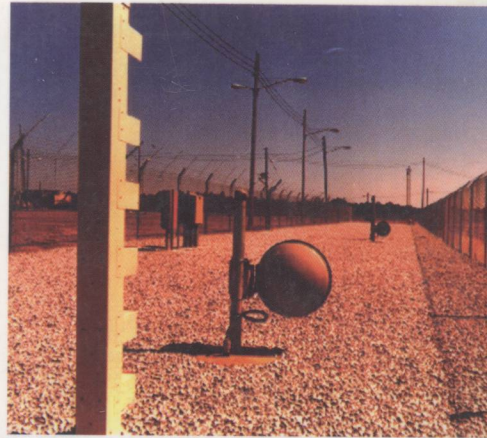


The Design and Evaluation of
**PHYSICAL
PROTECTION
SYSTEMS**



Mary Lynn Garcia

SECOND EDITION

C913
G216
E-2

The Design and Evaluation of Physical Protection Systems

Second Edition

Mary Lynn Garcia, CPP

Sandia National Laboratories



E2008001656



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier



Acquisitions Editor: Pamela Chester
Publisher: Amorette Pedersen
Marketing Manager: Marissa Hederson
Publishing Services Manager: Greg deZarn-O'Hare
Project Manager: Ganesan Murugesan
Cover Design: Joanne Blank

The US Government holds a nonexclusive copyright license in this work for government purposes. This book was authored by Sandia Corporation under Contract DE-AC04-94AL85000 with the US Department of Energy.

Copyright © 2008 by Butterworth-Heinemann



A member of the Reed Elsevier group

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

- ⊗ Recognizing the importance of preserving what has been written, Butterworth-Heinemann prints its books on acid-free paper whenever possible.

Library of Congress Cataloging-in-Publication Data

Garcia, Mary Lynn.

The design and evaluation of physical protection systems / Mary Lynn Garcia. – 2nd ed.
p. cm.

Includes bibliographical references and index.

ISBN-13: 978-0-7506-8352-4 (alk. paper)

ISBN-10: 0-7506-8352-X (alk. paper)

1. Security systems. I. Title.

TH9705.G37 2007

658.4'73—dc22

2007029245

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

The publisher offers special discounts on bulk orders of this book.

For information, please contact:

Manager of Special Sales

Butterworth-Heinemann

30 Corporate Drive, Suite 400

Burlington, MA 01803

Tel: 781-313-4787

For information on all Butterworth-Heinemann publications
available, contact our World Wide Web home page at: <http://www.bh.com>

07 08 09 10 11 10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

The Design and Evaluation of Physical Protection Systems

Second Edition

To the men and women, past and present, of the Security Systems and
Technology Center at Sandia National Laboratories, for 35 years of
exceptional service.

“In the future days, which we seek to make secure, we look forward to a
world founded upon four essential human freedoms . . . The fourth is
freedom from fear . . . anywhere in the world”.

Franklin D. Roosevelt, January 6, 1941

Preface

This book was first published in April 2001, just a few months before the horrific attacks of 9/11. I was personally gratified that this meant that our book was available to help address the security issues that arose out of these attacks. At the same time, we didn't include details that might have addressed this new threat motivation and capability. How could we—we never imagined that this sort of attack would be launched against civilian targets. The attacks of 9/11 are exactly the type of security event the approach described here is most effective for—high consequence, low probability events that require the most rigorous attention to detail we have available.

The world has gone through many changes since that time, particularly with respect to the security of its citizens. Wars in Afghanistan and Iraq provide a terrorist training ground; malevolent attacks on trains in Madrid, London and Mumbai, nightclubs in Bali, even a school in Beslan, Russia, are all examples of the tactics of emerging threats against ordinary citizens engaged in ordinary activities. Though the evolution of threat capability is not new, the renewed vigor of adversaries fighting for their ideology has caused a corresponding increase of security awareness by citizens—ask anyone who has flown since the attacks of 9/11. In this new environment, it is fitting that we revisit the principles and concepts of effective security and provide necessary updates.

Most of the changes in this version of the text are focused on new threat capabilities, legal and other changes that have occurred since 9/11, and discussion of

some emerging technologies that may be useful in the future. Related to emerging technologies, we have included a maturity continuum in Chapter 6 “Exterior Intrusion Detection” that may serve as a guide to the selection of new technologies to counter adversary threats. In addition, because the basic principles of security are the same regardless of the application, a new chapter that discusses the use of these principles in executive protection, ground transportation of cargo, and cyber systems (computers and networks) has been added. This version also includes a discussion of the use of neutralization (defeat of the adversary using force during an attack) as another performance measure of facility response and risk assessment.

This edition follows the recent release of another text on vulnerability assessment (VA) by this author (referenced in appropriate chapters throughout this work). The two books are meant to work together in a very complementary way. This book describes the overall process and approach, while the VA book describes how the process is applied to verify effective protection of assets.

As with the first edition, this book describes a problem-solving approach. It discusses defining and understanding the problem prior to designing the system, and describes methods used to evaluate the design before implementation. This book addresses the use of the many components that exist to support a security system, but it primarily shows how these elements are integrated to deliver an effective system. The process culminates in a risk assessment that predicts how well the protection

system performs and helps senior management quantify the remaining risk and inform their decisions. The core of the process is the discipline of systems engineering. All options must be considered for their cost and performance effectiveness and we implement those elements that are supported by science and engineering principles, test data, and meet customer objectives.

As with any work of this magnitude, there are a great many people to whom I owe a debt of gratitude. At Sandia they include Jake Deuel, Greg Elbring, Frank Griffin, Bruce Green, John Hunter, Willie Johns, Miriam Minton, Dale Murray, Cindy Nelson, Chuck Rhykerd, Charles Ringler, JR Russell, Steve Scott, Mark Snell, Regan Stinnett, Boris Starr, Basil Steele, James Stevens, Dave Swahlan, Drew Walter, Ron Williams, Tommy Woodall, and Dennis Miyoshi. The expert information presented in this text belongs to them; any errors are strictly mine. This assertion, though often repeated, is nonetheless sincere.

At Elsevier Butterworth–Heinemann, Pam Chester, Mark Listewnik, Jenn Soucy, Kelly Weaver, Greg deZarn-O’Hare, Ganesan Murugesan, and Renata Corbani quickly and competently handled the publishing process. I am also grateful to Mark Potok and the Southern Poverty Law Center for permission to use the map that appears in Chapter 3, “Threat Definition” and Don Utz at Kontek and David Dickinson from Delta Scientific for pictures in Chapter 11 “Access Delay.” Chapter 16 “Other Applications” required assistance from others outside of Sandia with specific expertise, and so my particular thanks to Joe Carlon and Dick Lefler for their expert guidance and input on executive protection, and Weston Henry for providing the section on cyber security. Finally, my special thanks to Doug, Fuzzy, and Kasey.

As with the first edition, I hope you find this book helpful.

Mary Lynn Garcia

Contents

PREFACE	xvii
CHAPTER 1 / DESIGN AND EVALUATION OF PHYSICAL PROTECTION SYSTEMS	1
Safety Versus Security	2
Deterrence	2
Process Overview	3
PPS Design and Evaluation Process—Objectives	3
PPS Design and Evaluation Process—Design PPS	5
PPS Design and Evaluation Process—Evaluate PPS	5
Physical Protection System Design	6
PPS Functions	6
Detection	6
Delay	7
Response	7
Design Goals	7
Design Criteria	8
Performance Measures	8
Analysis	8
Physical Protection System Design and the Relationship to Risk	9
Summary	10
References	11
Questions	11
PART ONE / DETERMINING SYSTEM OBJECTIVES	13
CHAPTER 2 / FACILITY CHARACTERIZATION	15
Physical Conditions	16
Facility Operations	16
Facility Policies and Procedures	17
Regulatory Requirements	18
Safety Considerations	18
Legal Issues	19
Security Liability	20
Failure to Protect	20
Overreaction	20
Labor/Employment Issues	20
Corporate Goals and Objectives	21

Other Information	21
Summary	22
Security Principle	22
References	22
Questions	23
 CHAPTER 3 / THREAT DEFINITION	 25
Steps for Threat Definition	26
List Threat Information	26
Outsiders	28
Insiders	28
Capability of Adversary	30
Adversary Tactics	31
Potential Actions	31
Collect Threat Information	32
Intelligence Sources	32
Crime Studies	33
Professional Organizations and Services	33
Published Literature and the Internet	33
Government Directives and Legislation	34
Organize Threat Information	36
Sample Threat Statements	37
Summary	39
Security Principle	40
References	40
Questions	40
 CHAPTER 4 / TARGET IDENTIFICATION	 43
Undesirable Consequences	43
Consequence Analysis	44
Targets	45
Techniques for Target Identification	46
Manual Listing of Targets	46
Logic Diagrams	46
AND Gate	48
OR Gate	48
Events	49
Primary Events	49
Transfer Operation	49
Vital Area Identification	50
Sabotage Fault Tree Analysis	51
Generic Sabotage Fault Trees	52
Location of Vital Areas	52
Summary	53
Security Principle	53
References	54
Questions	54

PART TWO / DESIGN PHYSICAL PROTECTION SYSTEM	55
CHAPTER 5 / PHYSICAL PROTECTION SYSTEM DESIGN	57
Physical Protection System Design	58
PPS Functions	59
Detection	59
Delay	60
Response	61
Relationship of PPS Functions	62
Characteristics of an Effective PPS	63
Protection-in-Depth	63
Minimum Consequence of Component Failure	63
Balanced Protection	64
Design Criteria	64
Additional Design Elements	65
Summary	66
Security Principles	66
Reference	66
Questions	66
CHAPTER 6 / EXTERIOR INTRUSION SENSORS	69
Performance Characteristics	69
Probability of Detection	69
Nuisance Alarm Rate	71
Vulnerability to Defeat	71
Sensor Classification	72
Passive or Active	72
Covert or Visible	73
Line-of-Sight or Terrain-Following	73
Volumetric or Line Detection	73
Application	73
Sensor Technology	73
Buried-Line Sensors	74
Pressure or Seismic	74
Magnetic Field	75
Ported Coaxial Cables	75
Fiber-Optic Cables	76
Fence-Associated Sensors	77
Fence-Disturbance Sensors	77
Sensor Fences	78
Electric Field or Capacitance	78
Freestanding Sensors	78
Active Infrared	79
Passive Infrared	80
Bistatic Microwave	80
Monostatic Microwave	81
Dual-Technology Sensors	82
Emerging Technology	82
Video Motion Detection	82
Passive Scanning Thermal Imagers	84

Active Scanning Thermal Imagers	85
Ground-Based Radar	85
Wireless Sensor Networks	86
Red/Blue Force Tracking	87
Maturity Model for Security Technologies	88
Perimeter Sensor Systems—Design Concepts and Goals	89
Continuous Line of Detection	89
Protection-in-Depth	90
Complementary Sensors	90
Priority Schemes	90
Combination of Sensors	91
Clear Zone	92
Sensor Configuration	92
Site-Specific System	92
Tamper Protection	93
Self-Test	93
Pattern Recognition	93
Effects of Physical and Environmental Conditions	93
Lightning Protection	95
Integration with Video Assessment System	95
Integration with Barrier Delay System	95
Exterior Sensor Subsystem Characteristics	96
Procedures	96
Summary	98
Security Principles	98
References	98
Questions	99
 CHAPTER 7 / INTERIOR INTRUSION SENSORS	 101
Performance Characteristics	101
Sensor Classification	103
Active or Passive	103
Covert or Visible	103
Volumetric or Line Detection	103
Application	103
Sensor Technology	104
Boundary-Penetration Sensors	104
Vibration Sensors	104
Electromechanical Sensors	105
Capacitance Sensors	107
Infrasonic Sensors and Passive Sonic Sensors	107
Active Infrared Sensors	108
Fiber-Optic Cable Sensors	108
Interior Motion Sensors	109
Microwave Sensors	109
Ultrasonic Sensors	111
Active Sonic Sensors	112
Passive Infrared Sensors	112
Dual-Technology Sensors	114
Video Motion Detection	115

Proximity Sensors	115
Capacitance Proximity Sensors	116
Pressure Sensors	117
Wireless Sensors	117
Miscellaneous Technologies	119
Effects of Environmental Conditions	119
Electromagnetic Environment	119
Nuclear Radiation Environment	120
Acoustic Environment	120
Thermal Environment	120
Optical Effects	120
Seismic Effects	120
Meteorological Effects	120
Sensor Selection	120
Procedures	121
System Integration	122
Summary	123
Security Principles	123
References	123
Questions	123
CHAPTER 8 / ALARM ASSESSMENT	127
Assessment Versus Surveillance	128
Video Alarm Assessment System	129
Camera and Lens	130
Basic Television Operation	130
Resolution	131
Resolution Limited Field of View	132
Types of Cameras	134
Additional Considerations	135
Image Device	136
Image Device Format	136
Lenses	137
Lens Format	137
Focal Length and Field of View	137
<i>f</i> -Number	138
Distance and Width Approximation	138
Maximum Usable Zone Length	139
Interior Assessment Zones	140
Camera Mounting/Support Structures	141
Lighting System	143
Camera Sensitivity	143
Scene Illumination	144
Parameters	144
Types of Lighting	145
Transmission System	146
Bandwidth	147
Line Loss	147

Signal Conditioning	147
Video Equalizers	147
Hum Clampers	147
Fiber-Optic Transmission	148
Video Switching Equipment	148
Video Recording	148
Characteristics	149
Video Monitor	149
System Compatibility	150
Video Controller	151
Additional Design Considerations	151
Site/Sector Layout	151
Video and Sensor Interference	152
Monitor Location	152
Construction	152
Alarm Assessment by Response Force	152
Integration with Safety Systems	152
Legal Issues	153
Camera Selection Procedures	153
Acceptance Testing	154
Summary	156
Security Principles	157
References	157
Questions	158
 CHAPTER 9 / ALARM COMMUNICATION AND DISPLAY	 161
Evolution of Alarm Reporting Systems	162
AC&D Attributes	162
Alarm Communication Subsystem	163
Physical Layer	165
Network Architecture	165
Security Considerations	167
Low-Level Protocols	167
Link Layer	168
Network Layer	168
Line Supervision and Security	168
Types of Supervision	169
Encryption Systems	170
Information Handling	171
Sensor Data Issues	171
Intelligent Alarm Analysis	172
Alarm Control and Display	173
Ergonomics—Human Factors	173
Points to Consider	174
Ergonomics—Graphical Displays	175
Assessment	178
Graphics Monitors	178
CCTV Monitors	179
Input Devices	179
Operator Interface	180

Offline Systems	180
Event Logs	180
Use of Databases	181
Event Printer	181
Supervisory Consoles	181
AC&D System Design	181
Interface with Entry Control Systems	181
Integration with Assessment Systems	182
System Security	182
Operator Loading	182
The AC&D Console as an Overload Source	183
Event Conditions	183
Consoles	184
Computers	184
Uninterruptible Power	184
Shared Components	184
Compatibility with Operational Procedures	184
Summary	185
Security Principles	185
Questions	186
 CHAPTER 10/ ENTRY CONTROL	 187
Personnel Entry Control	188
Personal Identification Number	188
Credentials	189
Photo Identification Badge	189
Exchange Badge	189
Stored-Image Badge	189
Coded Credential	189
Personnel Identity Verification (Biometrics)	192
Hand/Finger Geometry	193
Handwriting	194
Fingerprints	194
Eye Pattern	195
Voice	196
Face	197
Other Techniques	198
Personnel Entry Control Bypass	198
Contraband Detection	198
Manual Search	198
Metal Detectors	199
Package Search	201
Explosives Detection	201
Bulk Explosives Detection	202
Trace Explosives Detection	204
Chemical and Biological Agent Detection	207
Locks	208
Major Lock Components	208
Fastening Device	208
Strike	209

Hasps and Shackles	210
Coded Mechanism	210
Keyless Coded Mechanisms	210
Key Coded Mechanisms	211
Installation Considerations	211
System Integration and Installation Issues	212
Procedures	214
Administrative Procedures	215
Summary	216
Security Principles	216
References	216
Questions	217
CHAPTER 11/ ACCESS DELAY	219
Barrier Types and Principles	220
System Considerations	221
Aspects of Penetration	221
Perimeter Barriers	223
Fences	224
Gates	225
Vehicle Barriers	225
Structural Barriers	228
Walls	229
Doors	230
Standard Doors	231
Windows and Utility Ports	233
Roofs and Floors	235
Dispensable Barriers	236
Procedures	239
Summary	240
Security Principles	241
References	241
Questions	241
CHAPTER 12/ RESPONSE	243
General Considerations	244
Response Force Performance Measures	245
Contingency Planning	245
Joint Training Exercises	247
Use of Force	248
Training	248
Communication	249
Normal Use	249
Eavesdropping and Deception	250
Jamming	251
Survivability of the Radio Network	252
Alternate Means of Communication	252
Duress Alarms	253
Spread-Spectrum Systems	254

Interruption	255
Neutralization	255
Procedures	256
Summary	257
Security Principles	258
References	258
Questions	259
PART THREE / ANALYSIS AND EVALUATION	261
CHAPTER 13/ ANALYSIS AND EVALUATION	263
Adversary Paths	264
Effectiveness Measures	265
Quantitative Analysis	267
Critical Path	269
Qualitative Analysis	270
Summary	271
Security Principles	271
Questions	271
CHAPTER 14/ EASI COMPUTER MODEL FOR ANALYSIS	273
Quantitative Analysis Tools	273
EASI Model	275
The Input	275
Standard Deviation	277
The Output	278
Using the Model	278
EASI Examples	278
Critical Detection Point	280
Use of Location Variable in EASI	281
Adversary Sequence Diagrams	283
Site-Specific ASD	286
Summary	288
Security Principle	289
References	289
Questions	289
CHAPTER 15/ RISK ASSESSMENT	291
Risk Management Approaches	292
Risk Equation	292
Vulnerability Assessment Process	293
Risk Assessment	294
Performance Testing	296
Summary	297
Security Principle	297
Reference	297
Questions	297

CHAPTER 16/ PROCESS APPLICATIONS	299
Executive Protection	299
Determine Protection Objectives—Facility Characterization, Threat Definition, and Asset Identification	300
Protection Functions—Detection, Delay, Response Analysis	301
Ground Transportation	302
Determine Protection Objectives—Facility Characterization, Threat Definition, and Asset Identification	303
Protection Functions—Detection, Delay, Response Analysis	304
Cyber Systems (Computers and Networks)	306
Cyber Security Fundamentals	307
Determine Protection Objectives—Facility Characterization, Threat Definition, and Asset Identification	308
Sample Threat Spectrum	310
CPS Functions—Detection, Delay, Response Analysis	311
Summary	312
References	313
APPENDIX A / THREAT TABLES	314
APPENDIX B / NETWORK SITE SURVEY	317
APPENDIX C / EASI MODEL	319
GLOSSARY	325
INDEX	343