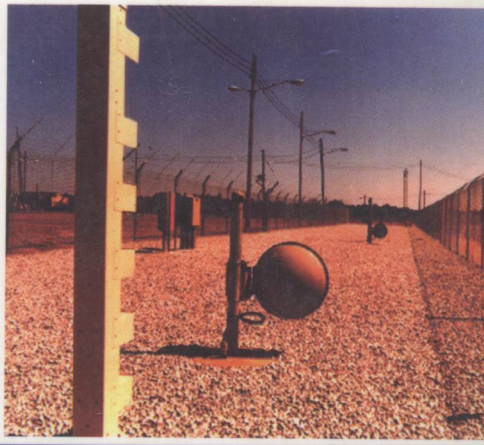
The Design and Evaluation of PHYSICAL PROTECTION SYSTEMS



Mary Lynn Garcia

SECOND EDITION

B
H

The Design and Evaluation of Physical Protection Systems

Second Edition

Mary Lynn Garcia, CPP

Sandia National Laboratories

ELSEVIER

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

Butterworth-Heinemann is an imprint of Elsevier

BH

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

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