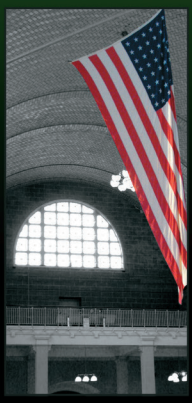
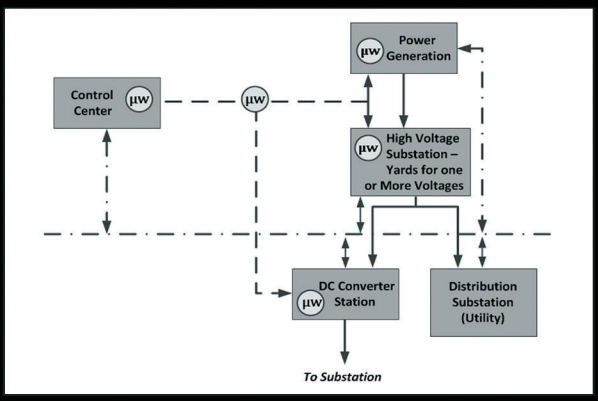
Critical Infrastructure System Security and Resiliency





Betty E. Biringer • Eric D. Vugrin • Drake E. Warren

CRC Press
Taylor & Francis Group

Critical Infrastructure System Security and Resiliency

Critical Infrastructure System Security and Resiliency

Betty E. Biringer
Eric D. Vugrin
Drake E. Warren

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2013 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20130308

International Standard Book Number-13: 978-1-4665-5751-2 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

…to the staff at Sandia National laboratories who have actively committed their research, motivations, innovations, and efforts to make our national critical infrastructure more secure and resilient.

© 2010 Taylor & Francis Group, LLC

Contents

List of Figures xiii
List of Tables xv
Foreword xvii
Acknowledgments xxi
About the Authors xxiii
Acronyms and Abbreviations xxv

Section I

SECURITY RISK ASSESSMENT

1 Introduction to Security Risk Assessment 3

Security Risk Assessment 5
Protection System Robustness 6
Security System Resiliency 6
System Approach for Security Risk Assessment 7
Determine Undesired Events, Associated Critical Assets, and Available Resources 8
Threat Analysis 8
Assess Likelihood of Initiating Event 8
Estimate Protection System Effectiveness 9
Assess Consequences for Undesired Event 9
Estimate Security Risk 9
Upgrade the Protection System to Be Robust against Undesired Event 10
Upgrade Security System to Be Resilient for Undesired Event 10
Summary 10
Reference 10

2 Undesired Events, Associated Critical Assets, and Available Resources 11

Critical Assets 11
Logic Model 12
Logic Gates 12

© 2010 Taylor & Francis Group, LLC

Transfer Operations 13
Primary Events 13
Resources 16
Summary 16
References 17

3 Threat Analysis 19

Malevolent Threats 19
Type of Adversary 23
Adversary Capability 24
Design Basis Threat 25
Natural Hazards 26
Hurricane 27
Earthquake 27
Tornado 27
Flood 27
Accidents 28
Summary 29
References 29

4 Likelihood of Initiating Events 31

Malevolent Threat 31
Outsider Threat 32
Insider Threat 34
Natural Hazard Threat 36
Accident Threat 36
Summary 38
References 38

5 Assess Consequences and Responses for Undesired Event 39

Reference Table for Consequences 39
Estimating Consequence Level for Undesired Events 41
Summary 42
Reference 42

6 Assessment of Protection System Effectiveness 43

Assessment of Protection System Effectiveness for Malevolent Threat 43
Adversary Scenarios 44
Effective Physical Protection System for the Malevolent Threat 46

© 2010 Taylor & Francis Group, LLC

Physical Protection System Effectiveness Assessment 48
Assessment Example 49
Protection System Effectiveness against Blast Attacks 52
Assessment Example 52
Mitigation of the Insider Threat 53
Cyber Protection System Effectiveness 55
Cyber Functions 56
Assessment Example 57
Effectiveness for Natural Hazards 58
Protection System Effectiveness Assessment Example 59
Protection System Effectiveness for Accidents 60
Assessment Example 60
Summary 62
References 62

7 Estimate Security Risk 63

System Approach for Security Risk Assessment 63
Determine Undesired Events, Associated Critical Assets, and Available Resources 64
Threat Analysis 65
Assess Likelihood of Initiating Event 65
Estimate Protection System Effectiveness 65
Assess Consequences for Undesired Event 67
Estimate Security Risk 68
Upgrade Protection System to Be Robust against Undesired Event 70
Upgrade Security System to Be Resilient for Undesired Event 72
Summary 72

Section II

EVALUATION AND DESIGN OF RESILIENT SYSTEMS

8 Motivating Infrastructure Resilience Analysis 75

References 78

9 Current State of Resilience Assessment 79

Definitions of Resilience 80
Domains 84

© 2010 Taylor & Francis Group, LLC

Assessment Processes 85
Structural Resilience Assessment Methodologies 86
Qualitative Assessments 86
Quantitative and Semiquantitative Indexes 87
Performance-Based Measurement 89
Seismic Resilience 90
Probabilistic Assessment 91
Economic Resilience 93
Hybrid Approaches 96
Gaps and Limitations 99
Endnotes 102
References 102

10 Infrastructure Resilience Analysis Methodology 105

Definition of Resilience 107
Measurement of Resilience Costs 108
Systemic Impact 109
Total Recovery Effort 111
Resilience Cost Calculation 112
Use and Interpretation of Recovery-Dependent Resilience Costs and Optimal Resilience Costs Quantities 114
Additional Notes on Calculation of Resilience Costs 115
Qualitative Structural Analysis 116
Absorptive Capacity 117
Adaptive Capacity 119
Restorative Capacity 121
Additional Notes on Resilience Capacities 123
Applying the Infrastructure Resilience Analysis Methodology 124
Summary 128
Endnote 129
References 129

11 Case Studies Using the Infrastructure Resilience Analysis Framework 131

Qualitative Resilience Analysis Case Study 132
Define Systems 132
Define Scenario 133
Perform Structural Analysis 134
Analysis Conclusions 138
Quantitative Resilience Analysis Case Study 138
Define Systems 139
Define Scenario 139

© 2010 Taylor & Francis Group, LLC

Define Metrics and Obtain Data 140
System Performance 140
Total Recovery Effort 142
Calculate Resilience Costs 143
Perform Structural Analysis 146
Absorptive Capacity 146
Adaptive Capacity 148
Restorative Capacity 150
Conclusions 151
Case Study on Optimizing Resilient Recovery Strategies 152
Define Systems 152
Define Scenario 153
Define Metrics 155
Obtain Data and Calculate Resilience Costs 157
The Rail Network Analysis System 158
Optimization 160
Simulation Results 161
Conclusions 165
Summary 166
Endnotes 167
References 168

12 Future Directions 171

References 173

Appendix A: Example Use of Fault Trees to Identify Critical Assets 175

Appendix B: Physical Protection Features Performance Data 179

© 2010 Taylor & Francis Group, LLC

List of Figures

Figure 1.1 Risk evaluation and system design process. 7

Figure 2.1 Fault tree development for disrupt electric power transmission example. 14

Figure 2.2 Fault tree development for impair/cause loss of substation 2—transfer 1. 15

Figure 4.1 Threat environment determination for malevolent threat—outsider. 33

Figure 4.2 Hypothetical threat environment results for example DBT. 34

Figure 4.3 Description of threat environment assessment for insider positions example. 35

Figure 4.4 Threat environment assessment for natural hazards example. 36

Figure 4.5 Threat environment assessment for accidents example. 37

Figure 5.1 Consequence estimation for loss of infrastructure mission using example reference table for consequences example. 41

Figure 6.1 Fault tree example. 45

Figure 6.2 Integration of detection, delay, and response functions. 47

Figure 6.3 Physical protection system effectiveness assessment example. 51

Figure 6.4 Blast mitigation effectiveness assessment example. 53

Figure 6.5 Insider threat assessment example. 55

Figure 6.6 Cyberprotection system effectiveness assessment example. 58

Figure 6.7 Protection system effectiveness assessment for natural hazards example. 60

Figure 6.8 Protection system effectiveness assessment for accidents example. 61

Figure 7.1 Risk Evaluation and System Design Process. 64

Figure 7.2 Logical combinations of protection system effectiveness and consequences to estimate security risk level. 69

Figure 9.1 Conceptual illustration of MCEER's seismic resilience measurement. 91

© 2010 Taylor & Francis Group, LLC

Figure 9.2 Measuring probabilistic resilience. 92

Figure 9.3 Static economic resilience. 93

Figure 9.4 Dynamic economic resilience. 94

Figure 10.1 Representation of systemic impact (a) and total recovery effort (b). 110

Figure 10.2 Infrastructure system performance and recovery activities comprise a feedback loop. 113

Figure 10.3 The IRAM resilience hierarchy. 117

Figure 10.4 Resilience analysis process. 125

Figure 11.1 Electric power outage contours. 133

Figure 11.2 Structural resilience analysis of hydrofluoric acid. 135

Figure 11.3 Structural resilience analysis of hydrochloric acid. 137

Figure 11.4 2008 estimated weekly plastics shipments. 141

Figure 11.5 Absorptive capacity resilience enhancement factors. 147

Figure 11.6 Adaptive capacity resilience enhancement factors: Impact of feature on railroads is assumed to be felt equally by both chemical groups. 148

Figure 11.7 Restorative capacity resilience enhancement factors. 150

Figure 11.8 Locations of Mississippi River crossings. 153

Figure 11.9 Locations of other Mississippi River crossings. 154

Figure 11.10 Rail network analysis system transportation analysis zones and centroids. 158

Figure 11.11 Representation of main lines in the national rail network. 159

Figure 11.12 Optimization process. 160

Figure 11.13 Optimal restoration schedule for damaged bridges. 163

Figure 11.14 Systemic impact summary for optimal restoration plan. 163

Figure 11.15 Restoration schedule assuming no cooperation among companies. 164

Figure 11.16 Systemic impact summary for independent restoration plan. 165

Figure A.1 Fault tree development for disrupt electric power transmission example. 176

Figure A.2 Fault tree development for impair/cause loss of substation 2—transfer 1. 177

© 2010 Taylor & Francis Group, LLC

List of Tables

Table 3.1 Hypothetical Threat Reference Table 21

Table 3.2 DBT for Demonstration Analysis Example 25

Table 3.3 Natural Hazards Threat Data 26

Table 3.4 Accident-Related Threat Data 28

Table 5.1 Reference Table for Consequences Example—Electric Power Transmission 40

Table 6.1 Malevolent DBT for Assessment Demonstration Example 44

Table 6.2 Reference Table for Assessing Physical Protection System Effectiveness 50

Table 6.3 Reference Table for System Effectiveness for Blast Effects 53

Table 6.4 Reference Table for System Effectiveness for Mitigation of the Insider Threat 55

Table 6.5 Reference Table for Assessing Cyber Protection System Effectiveness 57

Table 6.6 Reference Table for Assessing Protection System Effectiveness for Natural Hazards 59

Table 6.7 Reference Table for Assessing Protection System Effectiveness for Accidents 61

Table 7.1 P_E (1 – P_E), and Vulnerabilities for Malevolent Threats 66

Table 7.2 P_E, (1 – P_E), and Vulnerabilities for Natural Hazards 67

Table 7.3 P_E, (1 – P_E), and Vulnerabilities for Accidents 67

Table 7.4 Consequence Levels for Events 68

Table 7.5 Relative Security Risk Levels 69

Table 7.6 Effects of First System Upgrade Option (Make System Robust) on Security Risk Level Example 71

© 2010 Taylor & Francis Group, LLC

Table 7.7 Effects of Second System Upgrade Option (Reduce C) on Security Risk Level Example 71

Table 10.1 Commonly Used Systemic Impact Metrics 109

Table 10.2 Commonly Used Total Recovery Effort Metrics 111

Table 10.3 Resilience Capacity Characteristics 117

Table 11.1 Hydrofluoric Acid (HF) and Hydrochloric (HCl) Affected 134

Table 11.2 Chemical Products Included in the Analysis 139

Table 11.3 Systemic Impact and Total Recovery Effort Metrics 140

Table 11.4 Systemic Impact Calculations for Plastics Chemicals 143

Table 11.5 Systemic Impact Calculations for Organic Chemicals 144

Table 11.6 Total Recovery Effort Calculations for Plastics Chemicals 144

Table 11.7 Total Recovery Effort Calculations for Organic Chemicals 145

Table 11.8 Resilience Cost Calculations 146

Table 11.9 Repair Mode Statistics 155

Table 11.10 Variables Necessary for Systemic Impact Calculations 156

Table 11.11 Summary of Daily Flow Changes within Five-State Region with All Four Bridges Out of Service 162

Table 11.12 Systemic Impact Calculations 164

Table 11.13 Summary of Recovery Strategy Impacts 164

© 2010 Taylor & Francis Group, LLC

Foreword

Each of us makes risk calculations every day. Should I bring an umbrella in case it rains? Should I go to the gym? What type of car should I buy? What type of health or life insurance do I need? Similarly, cities across the country look at the risks and needs of their communities and weigh decisions regarding choices between hiring and cutting police officers, firefighters, and teachers. And at the national level, we must also prioritize what we protect by choosing which threats or hazards to focus our investments on, and to what degree. Today, as risk is pervasive in all that we do, so too are risk calculations central to how we live.

What is less common, and less established—but perhaps more important than ever in the context of fiscal constraints and limited resources—is how to best identify and prioritize the risks that we face, and in turn, make smart investments based on these priorities. In their book *Critical Infrastructure System Security and Resiliency*, Betty E. Biringer, Eric D. Vugrin, and Drake E. Warren have set a course for policy-makers and practitioners to answer these important questions. Moreover, they have helped to lay out a structure and approach for performing and utilizing risk assessments in a manner that extends beyond the theoretical and puts tools squarely in the hands of decision-makers and security experts for use today.

Risk assessments underlie homeland security, which is fundamentally about risk management. Since the founding of the Department of Homeland Security, experts have endeavored to better identify and distinguish higher from lower risks—a process known as *risk segmentation*. No family, town, or nation could afford to eliminate all risk, even if it were feasible to do so. Risk assessments enable risk segmentation, and thus in turn, help us focus our limited resources on our highest security concerns. We know, for example, the vast majority of cargo coming to the United States presents little to no risk. The question is where and how should we deploy security programs to maximize our ability to deter and detect maleficent activity, while also allowing legitimate trade to move rapidly through the system? The answer lies in our ability to segment cargo into high- and low-risk categories, and then scan or inspect all the high-risk cargo before it departs to the United States.

Pre✓, a relatively new pre-screening program run by the Transportation Security Administration (TSA), uses risk assessments on passengers who voluntarily participate to expedite low-risk travelers through security checkpoints

© 2010 Taylor & Francis Group, LLC

at U.S. airports. Because of the ability to segment the traveling public into lower and higher risk categories under this program, TSA security officers can now focus their attention and screening principally on the higher risk travelers, speeding travel for passengers, while enhancing overall security.

As important as these advances have been, however, such unilateral actions are not sufficient to deal with homeland security threats and vulnerabilities that transcend our borders. International collaboration is essential to deal with issues such as transnational organized crime, international terrorism, cyber security, and supply-chain security. And while such collaboration has dramatically increased in recent years, common solutions for risk mitigation are hard to identify when there is no universal agreement on what it means to be *at risk*. In facilitating development of a thus-far elusive common risk framework and approach to risk mitigation, this book comes at a critical time.

Beyond providing a useful general reference on risk assessments, it also highlights the essential, and often overlooked, role of risk calculations in the protection of critical infrastructure (CI)—those systems and assets, whether physical or virtual, such as the nation's electrical grid, banking network, energy distribution pipelines, communications network, transportation hubs and corridors, and emergency response systems, that modern economies have become increasingly dependent on to sustain our daily lives.

The incapacity or loss of critical infrastructures can have a significant and debilitating impact on national security, economic stability, and public health and safety. Yet despite its importance, we tend to take critical infrastructure for granted until something or someone disrupts it. Whether through terrorist acts such as the Yemen cargo bomb plot in October 2010 or natural disasters like the ash clouds from volcano Eyjafjallajökull's 2010 eruption, the tsunami that hit Tohoku, Japan in 2011, or Hurricane Sandy on the East Coast of the United States in 2012, we see the impact that disruptions can have on our daily lives and national economies.

Today, we are on the verge of the next leap forward in homeland security. Protecting critical infrastructure, a goal that the federal government has listed as a priority for the last two decades, has historically focused on *point* protection—protection of a physical asset at a specific location. As we assess risks to critical infrastructure, we can no longer emphasize physical protection of particular assets. We need also to acknowledge the reliance we have on information systems and the increasing interdependencies among the digital and physical worlds. Consequently, we must look to strengthen the security and resilience of these infrastructures as a *system* in order to truly safeguard our nation against threats.

The pages that follow represent a significant contribution to the science of critical infrastructure protection and resilience. The authors bring decades of experience drawn from our national requirement for a failsafe and

© 2010 Taylor & Francis Group, LLC

secure nuclear weapons arsenal. Their systems analysis approach provides a high-level, practical analytical framework that public and private sector owners and operators of critical infrastructure can use to better understand and evaluate infrastructure security strategies and policies. It represents a vital contribution to improving the safety, security, and resilience of our nation's infrastructure and to strengthening the broader homeland security enterprise.

David Heyman
Assistant Secretary for Policy
U.S. Department of Homeland Security

© 2010 Taylor & Francis Group, LLC

Acknowledgments

The authors are extremely grateful for the outstanding support of the team of people who made this book possible. The technical publication effort led by Sharon L. O'Connor, the most professional and capable technical editor with vast knowledge of security risk assessment and resiliency, ensured a timely and quality product. Sharon's contributions and efforts are sincerely appreciated, as well as those of Rebecca J. Horton, the graphics artist who created the professional graphics. Melissa D. Biringer, American Institute of Architects, is especially thanked by her mother for the favor of designing the book cover.

We would like to recognize the subject matter experts who provided technical review of the manuscript. The valuable suggestions and collaborations of John Darby, Mark Snell, Tom Goolsby, Heidi Ammerlahn, Steve Conrad, and William Plummer of Sandia National Laboratories are much appreciated. Mark Turnquist from Cornell University and Chris Camphouse from Sandia National Laboratories have been frequent collaborators and contributed to the advancement of mathematical resilience modeling; their contributions can be seen most clearly in the resilience case study of the U.S. freight rail network. We sincerely thank David Heyman for writing the Foreword, and Leonard Joseph, Matt Fuchs, and Matt Kangior for shepherding the Foreword through the review and approval process at the Department of Homeland Security.

This effort would not have been possible without the programmatic support of the management and staff at Sandia National Laboratories. Our gratitude is expressed to Ron Moya, director of the Critical Asset Protection and Security Center, and managers Carla Ulibarri, Pablo Garcia, Lillian Snyder, Ray Trechter, Howard Hirano, J.R. Russell, and Dan Rondeau.

We also want to extend appreciation to the many government sponsors and agencies that provided essential funding to the research projects that led to the development of the technical material for this text. The list of sponsors includes the Department of Energy, The Interagency Forum for Infrastructure Protection, the Department of Homeland Security, and the Sandia National Laboratories' Laboratory-Directed Research and Development program.

Finally, we thank our families for their stalwart support. Infrastructure security work can require extended work hours and absences from home. The encouragement and forbearance that we receive from our families during these absences make our professional endeavors possible.

© 2010 Taylor & Francis Group, LLC