

Index

- Acronym list, 345–346
- Adversary capability, 56
 - collusion, 56
 - equipment, 56, 57
 - expected number in group, 56, 57
 - explosives, 57, 58
 - financial resources, 57, 58
 - intelligence gathering means, 56, 57
 - motivation, 56, 57
 - potential for collusion with insider, 57, 58
 - tactics, 56, 57
 - targets of interest, 56, 57
 - technical skills/knowledge, 57, 58
 - transportation, 56, 57
 - weapons, 56, 58
- Adversary sequence diagrams (ASDs), 90, 91, 132, 154, 303
 - adjacent physical areas, 92
 - adversary paths, 91
 - jump feature, 306–307
 - path elements, 94, 304
 - physical areas, 304
 - protection layers, 92
 - protection system features, 304
 - contraband detection, 95
 - delay features, 94
 - detection features, 94
 - detection (with assessment), 94
 - entry control, 94
 - sabotage analysis, 93–94
 - system features, 92
 - theft analysis, 94
- Adversary spectrum, 53
 - hypothetical adversary spectrum summary, 59–61
- Adversary strategies, 88
 - critical assets for strategies, 90
 - most-vulnerable scenario, 96
 - critical asset, 96
 - path elements, 96
 - PPS effectiveness, 96, 97
 - functions of detection, delay, and response, 97
 - integrated functions, 97
 - undesired event, 96
 - most-vulnerable strategy, 88
- Asset prioritization, 83
 - prioritization matrix, 84
 - threat potential (likelihood of attack), 84
 - consequence, 84
 - undesired events, 84
- Audit, 16, 38
- Authentication, 15, 37
- Authorization, 15, 38
- Collusion threat, 56
- Conditional risk, 7
- Consequence analysis, 11, 75
 - consequence categories, 12,
 - consequence definitions, 12, 76
 - consequence severity level, 12
 - criteria, 76
 - estimating consequences for undesired events, 77–80
 - reference table of consequences, 75
- Consequence of successful adversary attack, 7
- Contingency protection system
 - upgrade, 173
- Critical assets, 40, 42
- Critical infrastructure, 4
- Cyber protection system, 37, 87
 - audit function, 38, 109, 115
 - intrusion detection system, 112
 - monitors for access control, 112
 - review of traffic data, 112

- scanners, 112
- virus protection, 112
- authentication function, 37, 109, 115
 - biometric authentication, 111
 - encryption techniques, 110
 - passwords (weak and strong), 110, 115
 - smart cards or tokens, 110
 - two-factor authentication, 110
- authorization function, 38, 109, 111, 115
- Cyber-protection system effectiveness, 88, 106, 113, 115
 - assessment, 107
 - availability, 106
 - confidentiality, 106
 - critical asset, 114
 - cyber-path diagram, 107
 - access points, 107
 - electronic links, 107
 - exterior electronic boundary, 107
 - functions, 108 (*see also Cyber-protection system*)
 - audit, 38, 109, 115
 - authentication, 37, 109, 115
 - authorization, 38, 109, 111, 115
 - integration of, 113, 115
 - integrity, 106
 - vulnerabilities, 112, 114
 - access control monitoring, 113
 - introduction of malicious code, 112
 - patches, 112
 - site-specific, 114
- Demonstration of the security risk assessment and management process, 189
 - blast effects analysis, 265–269
 - building fault tree, 208–212
 - consequence definitions, 229
 - consequences, 228, 230–239
 - critical assets, 207, 209, 213–214
 - cyber protection system
 - effectiveness, 259–265
 - example building, 197
 - facility characterization, 195
 - impact analysis, 286–288
 - insider threat severity, 227
 - management decisions, 296–297
 - physical protection system
 - analysis, 246–2579
- presentation package (to management), 289–295
- prioritization analysis, 239–244
- risk estimates, 271–273
- risk reduction, 273–285
 - consequence mitigation
 - upgrades, 282–284
 - cyber protection upgrades, 281–282
 - physical protection
 - upgrades, 274–281
- screening, 192
- threat, 215, 217 (table)
- threat potential/likelihood of
 - attack, 215, 219–226
 - undesired events, 207
- Design threat, 173
- Detection, 14
- Delay, 14, 95
- DHS, 51
- Effective protection system, 14
 - cyber system, characteristics of, 15
 - physical system, characteristics of, 14
 - relation to system ineffectiveness, 13
 - vulnerabilities, 13
- Effectiveness analysis complex protection systems, 100, 309
 - area traversal times, 311
 - completed example, 315–327
 - effectiveness factors, 310
 - instructions, 309–315
 - qualitative estimate, 100
 - response effectiveness, 312–313
 - system features for buildings, 315
- Effectiveness analysis simple protection systems, 99
 - inspection, 99
- Facility characterization, 9, 31
 - critical assets, 9, 31
 - cyber system description, 9
 - mission of building, 9
 - physical description, 9, 31
 - protection objectives, 9, 31
 - security concerns, 9
 - undesired events, 9, 31, 32
- Facility description, 33
 - cybersystem, 33, 34
 - facility operations, 33, 34
 - physical details, 33
 - restrictions, requirements, limitations, 33

- safety protection systems, 33
- security protection systems, 33, 35
- workforce description, 33
- Fault tree, 297
 - analysis, 297
 - 'AND' gate, 40, 41
 - completeness, 297
 - Fault Tree Handbook, 42
 - gate symbols, 299
 - intermediate events, 298
 - miscellaneous symbols, 300
 - 'OR' gate, 40, 41
 - primary events, 298
 - basic events, 298
 - developed event, 298
 - external event, 298
 - symbols, 298–299
 - undeveloped event, 298
 - site-specific, 43
 - top event, 297, 298
 - transfer operation, 41
- Fault tree for buildings (generic), 40, 297, 300
 - compromise health and safety of occupants, 301
 - compromise structural integrity of building, 301
 - disable/misuse emergency systems, 302
 - disable/misuse HVAC, 302
 - disable/misuse information system, 302
 - disable/misuse physical utilities, 301
 - disrupt normal work operations, 300
 - disruption of building mission, 300
- FBI, 53
- Final report, 166–171
 - Consequence analysis, 166, 168
 - executive summary, 166, 167
 - impact analysis, 167, 170
 - introduction, 166, 167
 - report overview, 171
 - risk estimation, 167, 169
 - risk reduction strategies and packages, 167, 170
 - supporting documentation, 167, 171
 - system effectiveness assessment, 166, 169
 - threat analysis, 166, 168
- Garcia, Mary Lynn, 36, 95
- Gelles, Michael G., 338
- Glossary, 347–350
- Homeland Security Advisories and Homeland Security Information Bulletins, 52
- IFIP, 5, 51
- Impact analyses, 165
- Information protection, 19
- Insider threat, 54, 55, 69, 329
 - background check, 337
 - collusion, 56
 - definition, 333
 - detection of malevolent actions, 340
 - detection of misuse or unauthorized activity, 340
 - deterrence, 338
 - employment positions, 334
 - entry/exit control for the insider, 340
 - gaps in protection, 341, 342, 343
 - insider access, 336
 - insider advantages, 334
 - insider authority, 336
 - insider knowledge, 336
 - insider motivations, 334
 - insider threat spectrum, 334
 - integrated protection system to mitigate, 329, 330
 - integration of effective security features, 339
 - legal and political issues, 329
 - logic tree, 332
 - 'AND' gate, 332
 - 'OR' gate, 332
 - transfer operation, 332
 - minimization of opportunity for malevolent acts, 339
 - operations security, role of, 341
 - personnel screening, 70,
 - for high-risk positions, 339
 - pre-employment screening, 337
 - proper response to malevolent acts, 341
 - protection features for, 336
 - protection goal, 338
 - protection system upgrades, 343
 - security awareness role, 338
 - undesired events, 331
- JTTF, 51
- Likelihood of attack, 7
- Management presentation package, 18, 165

- Management presentation package,
 - (*continued*)
 - briefing, 166
 - risk reduction, 17
 - packages, 18
 - impacts, 18
 - security risk estimates, 18
 - threat description, 18
- Military Standard 882D, 12, 77
- National Security Threat List, 53
 - Country Threat List, 53
 - Issues Threat List, 53
- National Threat Center, 53
 - Public Access Center Unit, 53
 - Terrorist Watch and Warning Unit, 53
 - Threat Monitoring Unit, 53
- Outsider threat, 54
 - collusion, 56
 - criminals, 54
 - extremists, 54
 - foreign intelligence personnel, 55
 - psychotics, 55
 - terrorists, 54
 - threat potential estimation (likelihood
 - of attack), 62
 - vandals, 55
- PDD63, 5
- Personnel screening, 70
- Physical protection system, 35, 87
 - detection, 35
 - delay, 36
 - effectiveness, 88
 - response, 37
 - features, 304
 - contraband detection, 95
 - delay features, 94
 - detection features, 94
 - detection (with assessment), 94
 - entry control, 94
- Protection objectives, 9, 31, 44, 87
- Protection system effectiveness, 87, 90, 96, 97
 - ASD, 90, 91, 305 *see also Adversary sequence diagrams*
 - detection and delay values, 90
 - most-vulnerable scenario, 90, 96
 - critical asset, 96
 - path elements, 96
 - PPS functions, 97
 - detection, delay, and response, 97
 - integrated functions, 97
 - relationships of, 98
 - Adversary Task Time, 98
 - system effectiveness analysis, 132
 - undesired event, 96
 - upgraded system, for the, 154
- Protection system effectiveness
 - worksheets, 309
- Reference Table of Consequences, 24, 51, 75
- Response, 14, 37
- Restrictions, requirements, limitations, 39
- Risk assessment report, 165
- Risk assessment team, 175
- Risk decisions, 4
- Risk management, 165
 - risk acceptance, 172
 - risk avoidance, 171
 - risk reduction, 172
 - risk spreading, 172
 - risk transfer, 172
- Risk management decisions, 165
- Risk parameters, 7
- Risk reduction, 154
 - ASDs, 154
 - reducing the consequences, 154
 - upgrading the protection system, 154
- Risk reduction recommendations, 165
- Risk reduction strategies, 17, 127
 - combination of, 148
 - comparing baseline system risk to
 - upgraded system risk, 156
 - “deterrence,” 127
 - impacts of, 153
 - building- or facility-specific, 153
 - strategies to mitigate
 - consequences, 132, 134
 - construction hardening, 133
 - alternate strategies, plans, 137
 - barriers, rigid and
 - energy-absorbing (frangible), 134
 - blast design basis threat, 133
 - blast effects, 133
 - building structural members, 134
 - characteristics, shape,
 - energy-release efficiency, and quantity of explosive material, 138

- computer calculations, 137
- computer simulation
 - ZAPOTEC, 138
- controlling vehicle access, 137
- distance of explosive from
 - target, 138
- explosive blast effects, generic
 - table of (ATF), 139
- finite-element-based computer simulation, 138
- graphs of blast-effect curves, 139
- hydrodynamic code CTH, 138
- mode of building failure, 135
- obstructions, 134
- orientation, 134
- preliminary structural
 - analysis, 136
- protection from explosive
 - attack, 136
- single points of failure, 135
- site features, 134
- standoff distance, 137
- structural dynamics code
 - PRONTO 3-D, 138
- technical description of structure
 - under attack, 138
- effects of the consequence reduction
 - features, 155
- emergency planning, 133, 145
 - early warning systems, 145
 - emergency action plans, 145
 - evacuation from premises, 145
 - first responders, 147
 - law enforcement tactics, 146
 - local support agreements, 147
 - temporary security response
 - force, 146
- optimized recovery, 133, 134, 143
 - backup and alternative
 - projects, 143
 - customer agreements, 144
 - supervisory control and data
 - acquisition (SCADA)
 - function, 143
- redundancy, 133, 141
 - backup systems, 141
 - inventory and stockpile
 - planning, 141
 - support agreements, 142
- Reference Table of
 - Consequences, 155
 - strategies to increase protection system
 - effectiveness, 129
 - authentication, authorization, audit
 - function upgrades and
 - integration, 129
 - cyber protection system upgrade
 - features, 131
 - cyber-protection system
 - upgrades, 129
 - detection, delay, response function
 - upgrades and integration, 129
 - physical protection system upgrade
 - features, 130
 - physical protection system
 - upgrades, 129
 - strategies to reduce security risk, 127
- Risk reduction upgrade packages, 17
 - comparison of relative costs associated
 - with upgrade packages, 158
 - costs, 157
 - impact analysis, 18, 157
 - impact on operations or schedules, 159
 - impact on public opinion, 160
 - relation to site-specific
 - vulnerabilities, 17
 - site-specific concerns, 160
- Sabotage analysis, 306
- Sandia National Laboratories, 5, 52
- SCADA, 37
- Screening analysis, 23
 - consequence criteria, 24
 - consequence parameter, 24
 - consequence categories, 24
 - levels of consequence, 24
 - Reference Table of Consequences, 24, 75
- Security risk, 8
 - assessment and management process
 - analysis of impacts imposed by risk
 - reduction upgrade
 - packages, 177, 184
 - comparison of estimated risk level to
 - threshold, 176, 183
 - consequence analysis, 176, 180
 - facility characterization, 175, 177
 - presentation to management, 177, 185
 - risk estimation, 121, 127, 176, 182
 - risk management decisions, 177, 185
 - risk reduction strategies, 176, 183

- Security risk, *(continued)*
 - system effectiveness
 - assessment, 176, 180
 - threat analysis, 175, 178
 - conditional risk, 122
 - equation, 8
 - estimation, 16
 - parameters, 121
 - consequences of adversary success, 121, 127
 - likelihood of adversary attack, 121, 127
 - system ineffectiveness, 8, 121, 127
 - process, 8, 19
 - security risk value, 122
 - traditional risk equation, 5
- Security risk estimates, 165
- Security system performance assessment, 16
- Site-specific fault tree, 43, 87
- Theft analysis, 308
- Threat analysis, threat potential,
 - likelihood of adversary attack, 10, 49, 161
 - adversary capability, 11
 - adversary history/intent, 11
 - design threat, 161
 - factors
 - adversary capability, 63, 64
 - adversary intent/history, 63, 65
 - relative attractiveness of asset to adversary, 63, 65
 - process, 50
 - project-specific threat, 161
 - relative attractiveness of asset to adversary, 11
 - revised threat, 161
 - sources of information, 50
 - local and state sources, 51
 - national sources, 52
 - threat definition, 10
 - threat description, 10, 87, 165
 - threat potential for attack, 58
 - initiating event./safety studies, 58
 - estimating, 62–69

Threat Assessment, A Risk Management Approach, 338

Turner, James T., 338

US Treasury Bureau of Alcohol, Tobacco and Firearms (ATF), 139

Vulnerabilities, 104, 114

 - cyber, 130
 - physical, 130
 - specific, 13, 87, 104, 114, 130, 154

Vulnerability Assessment of Physical Protection Systems, 36, 95

Workforce description, 38

 - positions, 39
 - pre-employment background investigations, 39, 70