

# Index

---

- Absorption* heuristic, xvi, 163  
in fire protection domain, 252
- Adaptability  
a basic theme, 241  
for resilience, 241  
holistic treatment, 26  
in software, 179–180  
on Apollo 13, 70  
overview, 7
- Agents, role of in disruptions, 43–46  
hardware agents, 44  
human agents, 43–44  
multiple-agent disruptions, 45–46  
on Mars Polar Lander, 77  
on Nagoya, 77  
number of agents, 45  
single-agent disruptions, 45  
software agents, 44
- American Flight 191, Chicago O'Hare  
case history, 71–72  
*conflicting priorities* heuristic, 174  
deficient maintenance, 149, 205  
resilience aspects, 73
- Analytic methods, 122  
disruptions, for dealing with, 52–53  
position within resilience architecture, 15
- Apollo 11  
example of *human backup*  
heuristic, 41
- Apollo 13  
adaptability, 162, 167, 169–170  
case history, 69–70  
disruptions, 43, 56–57, 148–149  
functional redundancy, 138  
interelement collaboration, 176  
resilience, 160, 243  
resilience aspects, 70
- Architecting, xv, 30  
and the systems architect as a holistic  
capability, 139  
infrastructure architecting, see  
Infrastructure  
resilience architecting, 159–186
- Architecture, 5  
of an infrastructure, see Infrastructure
- Attributes of resilience  
adaptability, 242, see Adaptability  
capacity, see Capacity  
for the fire protection domain, 252  
flexibility, see Flexibility  
Flexibility for the fire protection  
domain, 253

- Attributes of resilience (*Continued*)
- interelement collaboration, see Interelement collaboration
  - interelement collaboration for the fire protection domain, 256
  - tolerance, see Tolerance
  - Tolerance for the fire protection domain, 254
- Automatic function* heuristic, 173
- Automated system monitoring* heuristic, 178
- Automatic train stop, Metrolink 111, 269–270
- Avoidance,
- first phase of resilience, 12–13, 123
  - in a disruptions context, 39–40
- Bhopal
- case history, 65–66
  - example of deficient culture, 182
  - example of deficient maintenance, 167, 174
  - example of deficient resilience, 11
  - example of the “Union Carbide factor,” 50
  - resilience aspects, 66
- Billings’ principles
- agreement with Grote rules, 183
  - automatic function* heuristic, 173
  - human monitoring* heuristic, 178
  - intent awareness* heuristic, 179–180
  - predictability* heuristic, 169
  - simplicity* heuristic, 170
  - use in aviation domain, 160, 229, 242
- Blue Origin
- private space vehicle, 96
  - photo, 97
- Boundaries
- graphical view, 72
  - organizational and contractual, 103, 147
  - system boundaries, see Systems Approach
- Boxer, Senator Barbara, 269
- Brittleness, 1, 151
- Buffering, a component of capacity, 163
- Cab signaling, Metrolink 111, 270
- California Public Utilities Commission, 265
- Capacity
- absorption and margin, xvi, 56
  - an attribute of adaptability, 123, 162–167
  - cost based on capacity, see Cost
  - deficient on Metrolink 111, 87
  - effect on resilience, 242
  - in fire protection domain, 252
  - lack of on Concorde, 85
  - of Metrolink system, 265–266
- Capabilities, 121–150
- capability drivers, 122–123
  - type of system, 122. See also System types under System
  - type of disruption, 122–123. See also Disruptions
  - resilience phases, 123. See also Phases of resilience
  - resilience attributes, 123. See also Attributes of resilience
  - capabilities, depth of, 123–124
  - capabilities overview, 24–27
  - managerial capabilities, 124–137
    - anonymous reporting, 125
    - audits, 127
    - communications lines, other, 126
    - corrective action, 133–134
    - cost management, 134–135
    - cultural oversight, see Culture
    - decision making, 132–133, 187
    - governance, see Governance
    - humans in a cultural context, see Culture
    - independent reviews, see Independent reviews
    - infrastructure design, see Infrastructure
    - interelement collaboration, See Interelement collaboration
    - managerial oversight, 124
      - position within resilience architecture, 15
      - position within resilience architecture, 15
    - regulatory environment, 135–136. See also Environment, regulatory
    - risk management, 129–132
      - risk and culture, see Risk denial paradigm
    - schedule management, 134
    - supplier management, 136–137
    - training for humans on the sharp edge, see Training
    - training, education and self-discovery, see Training, see Self-Discovery
    - vertical communications, 126
    - work environment, 135
  - position within resilience architecture, 15
  - technical capabilities, 137–150
    - analytic methods, see Analytic methods
    - architecting, see Architecting
    - expertise, see Expertise
    - holistic approach, see Holistic approach
    - interface management, see Interfaces
    - manufacturing, see Manufacturing
    - operations, see Operations

- position within resilience architecture, 15
- reliability, see Reliability
- requirements, see Requirements
- safety, see Safety
- software, see Software
- technical management
- technology management
- Case Histories, 55–89
  - American Flight 191, see American Flight 191, Chicago O’Hare
  - Apollo 13, see Apollo 13
  - Bhopal, see Bhopal
  - case for case histories, 56–57
  - case histories provide clues, 241
  - Challenger, see Challenger
  - Chernobyl, see Chernobyl
  - Clapham Junction, see Clapham Junction
  - Columbia, see Columbia
  - Comet, see Comet
  - Concorde, see Concorde
  - Flixborough, see Flixborough
  - Helios 522, see Helios 522
  - Japan Air Lines JL 123, Mount Osutaka, see Japan Air Lines JL 123, Mount Osutaka
  - Jésica Santillán, see Jésica Santillán
  - Katrina, see Katrina
  - King’s Cross Underground Station, see King’s Cross Underground Station
  - Mars Climate Orbiter, see Mars Climate Orbiter
  - Mars Polar Lander, see Mars Polar Lander
  - MetroLink 111, see MetroLink 111 Accident,
  - Nagoya, see Nagoya
  - New York Power Restoration, see New York Power Restoration
  - Phillips 66 Accident, see Phillips 66 Accident
  - Piper Alpha, see Piper Alpha
  - Seveso, see Seveso
  - Sioux City, see Sioux City
  - Tacoma Narrows Bridge, see Tacoma Narrows Bridge
  - Texas City-1947, see Texas City-1947
  - Texas City-2005, see Texas City-2005
  - Three Mile Island, see Three Mile Island
  - TWA 800, see TWA 800
  - US Airways 1549, see US Airways 1549
  - ValuJet, see ValuJet
- Challenger
  - case history, 58–59
  - disruptions, 6, 95–96,
  - culture aspects, 17, 99, 102, 234, 239
  - defects, 203
  - design focus paradigm, 114
  - lack of resilience, 11
  - lack of risk process, 182, 188
  - lack of safety process, 143
  - lack of verification, 43
  - reliability failure, 41
  - resilience aspects, 58
- Challenges of resilience architecting, 8–9
- Charismatic executive approach, 106
- Chernobyl
  - case history, 64–65
  - context-spanning* heuristic, 166
  - failure of requirements process, 140
  - multidisciplinary challenge, 2
  - operational errors, 147
  - predictability* heuristic, 169
  - resilience aspects, 65
  - root causes, 64
  - Swiss cheese model, 47
  - use of Billings’ heuristics, 19
- Clapham Junction
  - case history, 67–68
  - deficient maintenance, 149
  - resilience aspects, 68
- Capability Maturity Model (CMMI™), 107, 114, 121
  - as a measurement tool, 234
- Coaching approach, 108
- Cognitive lock
  - on Three Mile Island, 67
- Columbia
  - capabilities, 121
  - case history, 61–64
  - culture, 7, 17–18, 27, 96, 102, 234, 239, 241, 182–183
  - design-focus paradigm, 114
  - failure, 1, 11
  - probabilistic risk analysis, 200
  - recommendations, 62–63
  - resilience, 64
  - root causes, 63
  - unreliability, 43
  - visual surveillance opportunity, 173, 227
- Commercial Aircraft Safety Team (CAST), 152
- Comet
  - case history, 83–84
  - expertise, 17, 189
  - resilience, 8
- Communities of practice, 112, 128
- Complacency, 116
- Complementarity of resilience, 242
- Complex adaptive systems (CASs), 21, 151
- Complexity avoidance* heuristic, 170

- Concealment* heuristic, 175
- Concorde
  - case history, 84–85
  - example of small disruption, 40, 227
  - resilience aspects, 85
- Conflicting priorities paradigm, 61, 98, 104–105
  - on Metrolink incident, 267
- Considerations for resilience, see Resilience
- Constraint
  - external constraint paradigm, 103
  - organizational and contractual constraint paradigm, 103, 148
- Contracts, 25, 240
- Corrective actions, 94
- Context-spanning* heuristic, 166–167
  - in fire protection domain, 253
- Cost, 211–223
  - cost analysis limitations, 211
  - cost analysis optimism and pessimism, 212–213
    - heuristics as source of pessimism, 213
    - human error as source of optimism, 212–213
    - unpredicted disruptions as source of optimism, 212
  - cost analysis viable approaches, 213–218
    - cost based on capacity, 216–217
    - cost based on human errors in hospitals, 216
    - cost based on probability of mishap, 216
    - cost based on quantifiable measures, 215–218
    - cost based on reliability, 215–216
    - cost-benefit analysis, 25
    - FAA cost approach, 214–215
  - cost and schedule margins, 108
    - bottom-up estimates, 117
    - cost and schedule pressures, 189. See also Risk
  - cost management, 6, 11
  - implementing a cost plan, see Implementation
  - implementing with high benefit-to-cost ratio, see Implementation
  - low-cost approaches, 123, 218–220
    - aerospace costing, 220
    - civil infrastructure costing, 218–219
    - flood protection costing, 219–220
    - implementing low or negligible cost approaches, see Implementation
  - risk-based costing, 220–223. See also Risk
    - cost optimization, 221
    - cost control, 221–222
    - potential cost savings of resilience, 221
- Critical infrastructure protection, 2, 151
- Cross-scale interactions, 41
- Cultural change approaches
  - charismatic executive, see Charismatic executive approach
  - coaching, see Coaching approach
  - cost and schedule margins, see Cost and schedule margins
  - communities of practice, see Communities of practice
  - management selection, see Management selection
  - rewards and incentives, see Rewards and incentives approach
  - socratic teaching, see Socratic teaching approach
  - standard processes, see Standard processes
  - teams, see Teams approach
  - training, see Training approach
- Cultural change case studies, 113
  - Royal Dutch/Shell case, see Royal Dutch/Shell
  - Xerox case, see Xerox
- Culture management, 109–110
  - independent reviews, 108, 188
- Culture, 91–119
  - and culture, see Governance
  - cultural aspect of the Metrolink 111 system, 267
  - cultural change* heuristic, 183
  - cultural environment, 33, 240–241
  - culture management* heuristic, 183
  - defined, 91
  - difficulty of measurement, 234
  - element of resilience architecture, 27–28
  - factor in accidents, 55
  - flexible culture, 93
  - implementing a resilience culture, see Implementation
  - leadership principles, see Leadership principles
  - learning culture, 93
  - managerial responsibility, 26
  - objective assessment, 114
  - overview, 7
  - paradigms, positive and negative, see Paradigms
  - position within resilience architecture, 15
  - reporting culture, 92
  - resilience, the culture element, 92, 242
- Cultural end state, 92–94
  - preoccupation with failure, 92

- simplification of failures, reluctance, 92
- sensitivity to operations, 92
- reporting culture, see Culture
- commitment to resilience, 93
- learning culture, see Culture
- expertise, deference to, 94
- flexible culture, see Culture
  
- Decision making, 254
- Deference to expertise and a flexible culture, see Cultural end state
- Department of Defense Architectural Framework (DODAF), 23, 151
- Department of Environment, Food and Rural Affairs (Defra)
  - measuring capacity for flood control, 217
  - cost of capacity for flood control, 217
  - flood protection resilience,
- Dependability, 243
- Deterrence* heuristic, 175
- Defects, anomalies vs. systemic, 94, 241. See also Near misses and Incidents
- Design-focus paradigm, 94, 98–99, 198
- Discovery launch decision, 94
- Disruptions, 39–53
  - agents, role of in disruptions, see Agents, role of in disruptions
  - component vs. system failures, 42
  - latent conditions, disruptions caused by, 43
  - law of large numbers, relevance to disruptions, See Law of large numbers
  - measuring unpredicted disruptions, see Measuring resilience
  - Metrolink 111 disruption, 261–263
  - N<sup>2</sup> diagram, multiple-agent, see N<sup>2</sup> diagram, multiple-agent
  - normal accident theory, see Normal accident theory
  - not root cause of an accident, 243
  - overview, 6, 28–29
  - position within resilience architecture, 15
  - predicted vs. unpredicted disruptions, 51–52
  - probability of disruption, 40, 123. See also Feynman observation
  - resilience implications, 52–53
  - system errors vs. symptoms, see Errors, system
  - Swiss cheese model. See Swiss cheese model
  - type A or disruptions of input
    - defined, 22, 28, 39, 57, 122
    - disruptions, 53, 113
    - environment, 36
    - on US Airways Flight 1549, 88
    - on Metrolink 111 accident, 261
    - threat to hardness heuristic, 165
    - threat to concealment heuristic, 175
  - type B or systemic disruptions of function, capability or capacity. See also F-22 Raptor
    - Bhopal, 65
    - defined, 4, 22, 39, 122
    - disruptions, 53, 57
    - human error, 100, 114
    - F-22 Raptors, 41–42
    - pilot errors, 28
    - unpredicted disruptions as source of cost
      - analysis optimism, see Cost
      - unreliability, disruptions of, 42–43
- Distancing paradigm, 59, 100
- Diversity* heuristic, 168–169
  - in fire protection domain, 254
- Domains
  - aerospace, 17, 214, 220
  - air traffic control, 128
  - civil infrastructure, 218
  - flood protection, 219–220
  - hospital, 127, 144, 188, 216, 235
  - railways, 8, 57, 87–88, 152, 157, 201, 229, 240, 259–272
  - fire protection, see Fire protection infrastructure
  - space, 17
  - nuclear power, 17
  - military, 17
  - commercial business, 17
  - river-dam, 17
  - stock market, 17
  - manufacturing, 17
- Drift correction* heuristic, 63, 66, 172–173
  
- Emergence, xvii, 30
- Engineering, xviii
- Environment, 33–36. See also Identification of system environment under Systems Approach
  - contractual, 34
  - cultural, 33
  - economic, 33
  - geopolitical, 35
  - organizational, 35
  - physical, 36
  - political, 34
  - regulatory, 33–34
- Epstein observation, 131. See also Risk

- Errors, system vs. symptoms, 55, 190
- Ethics paradigm, 99–100, 125
- Expertise
- as a leadership principle, 116
  - as a technical capability, 144–146
  - critical factor in Columbia, 63
  - deficient on Windscale, 74
  - deficient on Comet, 83–84
- Faulty signal theory, Metrolink 111, 261–262
- Federal Railroad Administration (FRA), 265
- Federation of systems, 21
- Feinstein, Senator Diane, 269
- Feynman, Richard,
- access to NASA data, 190
  - observation on the probability of failure, 40, 90–91, 197
  - theory of “common interest,” 102, 118, 239
- Filming of crew, Metrolink 111, 268
- Financial stability
- as a metric, 204–205
- Finger in the Dyke (the parable), vi, 118
- Fire Protection Infrastructure and Domain, 133, 249–257
- both stand-alone and system of systems, 228–229
- Flexibility
- as an attribute of adaptability, 123, 167–171
  - deficient on Metrolink 111, 266
  - effect on resilience, 242
  - in fire protection domain, 253
  - on network systems, 158
  - result of case histories, 56
- Flixborough
- case history, 70–71
  - deficient maintenance, 149
  - resilience aspects, 71
- Foreign object debris (FOD), 193–194. See also Defects, Near Misses and Incidents
- Functional redundancy* heuristic, 163–164
- as a holistic principle, 138
  - cost aspect, 219
  - in fire protection domain, 252–253
  - on US Airways Flight 1549, 89
- Galveston hurricane of 1900, 41
- General Code of Operating Rules (GCOR), 157, 260
- Global Earth Observation System of Systems (GEOSS), 35, 157
- Governance, 187–195
- and culture, 190
  - a management capability, 26
  - cross-checks
    - in hospitals, 188
    - for Piper Alpha, 193
  - implementing governance, see Implementation
  - position within resilience architecture, 15
  - responsibilities, 194–195
    - resilience node, 194
    - program system resilience team, 194–195
    - program management, 195
    - functional groups and integrated product teams (IPTs), 195
- Governments, federal and state, Metrolink 111, 264–265
- Graceful degradation* heuristic, 46, 172
- Hardness* heuristic, 165–166
- Helios 522
- case history, 86–87
  - lack of resilience, 243
  - resilience aspects, 86
  - a multiple-agent accident, 46, 49, 139
- Heuristics, xvi, 3, 30
- absorption*, see *Absorption* heuristic
  - automated system monitoring*, see *Automated system monitoring* heuristic
  - automatic function*, see *Automatic function* heuristic
  - complementarity of heuristics, 184
  - complexity avoidance*, see *Complexity avoidance* heuristic
  - concealment*, see *Concealment* heuristic
  - context of heuristics, 160–161
    - system type, 160. See also System resilience phase, 160–161. See also Resilience
    - type of disruption, 161. See also Disruptions
    - application domain, 161
  - context-spanning*, see *Context-spanning* heuristic
  - cultural change*, see *Cultural change* heuristic
  - culture management*, see *Culture management* heuristic
  - definition, xvi, 159–160
  - deterrence*, see *Deterrence* heuristic
  - diversity*, see *Diversity* heuristic
  - drift correction*, see *Drift correction* heuristic
  - functional redundancy*, see *Functional redundancy* heuristic

- graceful degradation*, see *Graceful degradation* heuristic
- hardness*, see *Hardness* heuristic
- heuristics defined, 159
- heuristics as source of cost analysis  
pessimism, see *Cost*
- heuristics vs. analytical methods, xvi
- hidden interaction*. See *Hidden interaction* heuristic
- human back-up*, see *Human back-up* heuristic
- human error as source of cost analysis  
optimism, see *Cost*
- human-in-control* heuristic, a sub-set of *Predictability* heuristic. See *Predictability* heuristic.
- human-in-the-loop*, see *Human-in-the-loop* heuristic
- human monitoring*, see *Human monitoring* heuristic
- informed operator*, see *Informed operator* heuristic
- inspectability*, see *Inspectability* heuristic
- intent awareness*, see *Intent awareness* heuristic
- interelement impediment*, see *Interelement impediment* heuristic
- knowledge between nodes*, see *Knowledge between nodes* heuristic
- loose coupling*, see *Loose coupling* heuristic
- margin*, see *Margin* heuristic
- measuring heuristics, see *Measuring resilience*
- mobility*, see *Mobility* heuristic
- neutral state*, see *Neutral state* heuristic
- organizational decision-making*, see *Organizational decision-making* heuristic
- organizational planning*, see *Organizational planning* heuristic
- paradigms vs. heuristics, 95
- physical redundancy*, see *Physical redundancy* heuristic
- predictability*, see *Predictability* heuristic
- prevention*, see *Prevention* heuristic
- regroup*, see *Regroup* heuristic
- reparability*, see *Reparability* heuristic
- reorganization*, see *Reorganization* heuristic
- retaliation*, see *Retaliation* heuristic
- risk aggregation*, see *Risk aggregation* heuristic
- risk culture*, see *Risk culture* heuristic
- simplicity*, see *Simplicity* heuristic
- small problem focus*, see *Small problem focus* heuristic
- Hidden interaction* heuristic, 52, 143, 177–178
- High-level problem paradigm, 95–96
- High reliability organizations (HROs), 12, 132
- Holistic approach, 138, 139  
defined, 30  
disruptions, for dealing with, 53  
essential for resilience, 26  
for recovery, 123  
holistic vs. analytic methods, xvi, ix  
position within resilience architecture, 15
- Humans  
*human back-up* heuristic, 168  
human error, 4, 147  
in FAA analyses, 212–213  
human error theory, Metrolink 111, 261  
*human-in-control* heuristic, a subset of *Predictability* heuristic, 174, 220  
*human-in-the-loop* heuristic, 168  
humans in the system, 187  
the paradox, 3  
humans and requirements, 140  
human-intensive systems, 12, 19–20, 23, 122, 176  
*human monitoring* heuristic, 178  
measuring human aspects of resilience, see *Measuring resilience*  
role of rules, 183  
value of human life, 214
- Iceberg theory, 56. See also *Measuring resilience*
- Implementation, 225–237  
capabilities, 225–228. See also *Capabilities architecting*, 226. See also *Architecting analytic capabilities*, 226. See also *Analytic methods advanced capabilities*, 227. See also *Analytic methods low or negligible cost approaches*, 227. See also *Cost*  
in high-consequence or high-risk systems, 227. See also *Risk with high benefit-to-cost ratio*, 228  
an infrastructure, 228–231. See also *Infrastructure an enterprise*, 228–231  
a civil infrastructure enterprise, 228–229  
a private enterprise, 229  
a product-centered enterprise, 229  
a public enterprise, 280  
an internal infrastructure, 230–231. See also *Infrastructure*

Implementation (*Continued*)

- a risk process, 231–232. See also Risk
  - a contractual process, 232.
    - Contracts in infrastructure systems, 232.
      - See also Infrastructure
    - Contracts for technological systems, 233
  - a measurement system, 233–235. See also Measuring resilience
    - development metrics, 233–235
    - operational metrics, 235. See also Operations
  - cultural initiatives
    - position within resilience architecture, 15
  - governance, 235. See also Governance
  - a resilience culture, 236. See also Culture
  - a cost plan, 236–237. See also Cost
  - Metrolink implementation, 270–272
- Incidents, 56. Also see Near misses
- Independent reviews, 188–190
  - for culture management, 108
  - scheduled, 189
  - special purpose, 189
- Independent supplier paradigm, 98
- Individual responsibility paradigm, 100
- Inevitability paradigm, 100–101
- Informal cost analysis paradigm, 97–98
- Information management
- Informed operator* heuristic, 176
- Infrastructure and infrastructure systems, 151–158
  - adaptability aspects, 7
  - architecture, 151–154
  - authority within, 153–154
  - civil infrastructure systems, 123
    - civil infrastructure costing, see Cost
  - architecting, 156
  - as a system of systems, 156–157, 240
  - brittleness aspects, 5
  - infrastructure systems, 22–24
  - integrated product teams (IPTs), 132, 152, 154–156, 176
  - interelement collaboration, see Interelement collaboration
  - network-based, 157–158
  - operational view, 23, 152
  - organizational view, 153
  - position within resilience architecture, 15
  - resilience infrastructure, 147, 240
- Inspectability* heuristic, 170
- Integrated product teams (IPTs), see Infrastructure
- Interaction between components, 243–244
  - on Helios 522, 86

- Intent awareness* heuristic, 179
- Interelement collaboration
  - as an attribute of adaptability, 175–179
  - cost aspect, 218
  - deficient on American Flight 191, 71
  - deficient on Clapham Junction, 67
  - deficient on Seveso, 74
  - effect on resilience, 242
  - enhanced by teams, 107
  - expanded from *cross-scale connectivity*
  - in case studies, 56
  - interelement impediment* heuristic, 137, 179
  - of an infrastructure system, 22, 44, 153
  - of the Metrolink 111 system, 266–267
  - on human-intensive systems, 122–125
  - superior on New York Power Restoration, 80, 163
  - superior on US Airways Flight 1549
- Interfaces, 244
  - as analytic or holistic, xvii
  - as source of brittleness, 244
  - deficient on Mars Polar Lander, 83
  - in hospitals, 86
  - interface management as a technical capability, 142
  - source of brittleness, 244
- Interoperability, deficient on Katrina, 82
- Janney coupling, 105
- Japan Air Lines JL 123, Mount Osutaka, 149
  - case history, 72
  - resilience aspects, 73
- Jésica Santillán, 125
  - case history, 85–86
  - resilience aspects, 85
- Just Culture, 94
- Katrina
  - as an infrastructure system of systems, 22, 29, 151–152
  - as a human-intensive system, 44
  - case history, 81–82
  - communications, 179, 218, 239
  - deficient adaptability, 162
  - deficient interelement collaboration, 175
  - deficient margin, levee height, 164, 184
  - disruption, 6–7
  - deficient leadership, 20, 41, 133, 229, 240
  - resilience, 82
  - use of teams, 107
- King's Cross Underground Station

- case history, 75–76
- deficient regulatory process, 34
- deficient risk process, 131
- resilience aspects, 76
- Knowledge between nodes* heuristic, 178, 251, 256
  
- Latent conditions, 43, 154. See also Disruptions.
  - within organizations, 55, 152
- Law of large numbers, 50–51
  - lottery example, 51
- Laws, 180
  - Ashby's law, 180
- Leadership principles, 114–118
  - commonality of interest, 118
  - communication, vertical and horizontal, 117
  - complacency, fight against, 116
  - cost and schedule estimates, bottom up, 117
  - expertise, deference, 116
  - management aspects, 118
  - metrics, trust in, 118
  - Nestlé example, 115
  - risk, focus on, 116
  - safety first, 115
  - systems view, adoption of, 116
- Loose coupling, see Tight and loose coupling
  
- Maintenance
  - as a metric, 204
  - as a technical capability, 149
  - deficient on American Flight 191, 71
  - deficient on Bhopal, 61
  - deficient on Japan Air Lines JL 123, 72
  - deficient on Phillips 66, 73
  - deficient on Piper Alpha, 60
- Management
  - attitude as a metric, 205
  - selection, 109
- Manufacturing
  - as a technical capability, 147
- Margin
  - in fire protection domain, 252
  - margin* heuristic, xvi, 164–165
  - work safety margin, 165
- Mars Climate Orbiter
  - as a two-agent disruption, 46
  - case history, 82–83
  - defects, 203
  - resilience aspects, 83
- Mars Polar Lander
  - as a *hidden interaction*, 177
  - as a multiple-agent disruption, 44–46
  - as a system failure, 42
  - as an undesirable interaction, 49
  - case history, 76–77
  - defects, 203
  - deficient intent awareness heuristic, 179
  - deficient use of *predictability* heuristic, 169
  - deficient software adaptability, 180
  - deficient tolerance attribute, 172
  - lack of resilience, 243
  - resilience aspects, 77
  - use of analytic methods, 52
  - use of teams, 155
- Mean time between failure (MTBF), 101. See also Reliability
- Measuring resilience, 197–209. See also Resilience measurement
  - approaches to measuring resilience, 199–207
    - accident metrics and commercial aircraft, 204–205
    - Massachusetts Institute of Technology (MIT) risk model, 200–201
    - metrics to manage an organization, 205–207
    - organizational resilience, 297
    - probabilistic risk analysis (PRA), 199–200, See also Risk
    - statistical prediction and the iceberg theory, 201–203
  - difficulty of measuring resilience, 197–199
    - heuristics, 198
    - human aspects, 198
    - unpredicted disruptions, 199
  - implementing a measurement system, see Implementation
  - measurements that are possible, 208–209
    - capacity, 208. See also Capacity
    - health care, 208–209
    - reliability, 208. See also Reliability
    - safety, 208. See also Safety
  - metrics, 15
- Memorandum of understanding (MOU)
  - As tool for interelement collaboration, 228, 232
- Metrics, see Measuring resilience
- Metrolink 111 accident
  - as a system of systems, 264
  - basis of case history, 57
  - case history, 87
  - communications aspects, 239
  - human error aspect, 243
  - infrastructure aspects, 152

- Metrolink 111 accident (*Continued*)  
 issue of control, 240  
 issue of responsibility, 229  
 resilience analysis, 259–272  
 resilience aspects, 88
- Metropolitan Transportation Authority (MTA), 8
- Mission assurance, 36
- Mobility* heuristic, 174
- Multidisciplinary challenge, 2
- Nagoya  
 case history, 77–78  
 defects, 203  
 deficient adaptability, 42–43, 162  
 deficient *intent awareness* heuristic, 19, 179  
 deficient *predictability* heuristic, 169  
 human error aspect, 6  
 lack of resilience, 243  
 multiple-agent aspect, 46  
 resilience, 78  
 software, 28, 44
- National Transportation Safety Board, 265
- Near misses, 56, 69, 241. See also Incidents defined, 202
- Negative synergy, 50
- Nestlé leadership principles, 115–116
- $N^2$  diagram, multiple-agent, 49–50
- Network-based infrastructures, 157
- Neutral state* heuristic, 171, 173, 254
- New model, self-discovery, 111, 236
- New York Power Restoration  
 adaptability of humans, 4, 7  
 as an infrastructure system, 22, 151–152  
 case history, 79–80  
 communications aspects, 218  
 complementarity of heuristics, 184  
*graceful degradation* heuristic, 172  
 inherent resilience, 160  
 insight into disruptions, 56  
 insight into recovery, 57  
 interelement collaboration, 125, 162–= 163  
*reorganization* heuristic, 167  
 resilience aspects, 80
- “Normalization of technical deviance,” see Paradigms
- Normal accident theory, 48
- Operations  
 as a metric, 204  
 as a technical capability, 147
- implementation of metrics, see Implementation
- operational view of an infrastructure, see Infrastructure
- Organizational decision-making* heuristic, 173–174, 220
- Organizational planning* heuristic, 174, 220
- Oversight, 187
- Panama, 139
- Parallel tracks, Metrolink 111, 267–268
- Paradigms, 94–105  
 best paradigm, 110–111  
 conflicting priorities, see Conflicting priorities paradigm  
 design-focus, see Design-focus paradigm  
 distancing, see Distancing paradigm  
 external constraint paradigm, see Constraint, external, paradigm  
 ethics, see Ethics paradigm  
 genesis of paradigms, 105–106  
 heuristics, vs. paradigms, 95  
 high-level problem, see High-level problem paradigm  
 independent supplier, see Independent supplier paradigm  
 individual responsibility, see Individual responsibility paradigm  
 inevitability, see Inevitability paradigm  
 informal cost analysis, see Informal cost analysis paradigm  
 “normalization of technical deviance,” 92  
 organizational and contractual constraint, see Constraint  
 paradigms, defined, 92  
 predictability, see Predictability paradigm  
 positive and negative paradigms, 92  
 program management, see Program management paradigm  
 random human error, see Random human error paradigm  
 risk denial, See Risk  
 safety analysis, see Safety analysis paradigm  
 Titanic effect, see Titanic effect  
 traditional paradigm change, see Traditional paradigm change paradigm
- Performance shaping factors (PSF)  
 in hospitals, 216
- Petroski lessons, 113–114
- Phases of resilience, 12–13, 123  
 avoidance, 13, 123  
 survival, 13, 123  
 recovery, 13, 123

- Phillips 66 accident  
 case history, 73  
 deficient maintenance, 149  
 resilience aspects, 74
- Physical redundancy* heuristic, 164  
 effect on cost, 215
- Pilot competence  
 as a metric, 204
- Piper Alpha  
 case history, 60–61  
 communications aspects, 125, 239  
 cross checks for, 193  
 defects, 203  
 deficient maintenance, 149  
 example of deficient resilience, 11  
 resilience aspects, 62
- Positive train control, Metrolink 111, 268–269
- Predictability* heuristic, 169–179. See also  
*Human-in-control* heuristic
- Predictability paradigm, 104
- Predicted disruptions, see Predicted vs.  
 unpredicted disruptions
- Predicted vs. unpredicted disruptions, 51–52
- Preoccupation with failure, 95
- Prevention* heuristic, 175
- Private enterprise, see Implementation
- Probabilistic Risk Assessment (PRA), 108, 149
- Process systems, 20
- Product-centered infrastructure systems, 18–19.  
 See also product-centered enterprise in  
 Implementation
- Program management paradigm, 101
- Protection  
 defined, 14  
 protection vs. resilience, 14, 219
- Public enterprise. See also Implementation  
 Federal Bureau of Investigation (FBI), 230  
 Federal Emergency Management Agency  
 (FEMA), 230  
 New York Port Authority, 230  
 National Guard, 230
- Quality, inspecting in, 188
- Random human error paradigm, 103–104
- Recovery, 12–13
- Regulation  
 deficient in Texas City – 2005, 59  
 deficient in King’s Cross, 75
- Reliability, 148–149
- Reluctance to simplify interpretations, 93
- Regroup* heuristic, 175
- Reorganization* heuristic, 167, 198
- Reparability* heuristic, 171
- Requirements  
 humans and requirements, 140  
 in breadth, 52, 141–142, 122, 149  
 in depth, 140–141, 122
- Resilience, system resilience, and resilience  
 engineering  
 aspects, ix  
 challenges, see Challenges of resilience  
 architecting  
 concept diagram, 14–16  
 considerations for resilience  
 adaptability, see Adaptability  
 culture, see Culture  
 laws, see Laws  
 prediction, see Measuring resilience  
 risk, see Risk  
 capabilities, see Capabilities  
 culture element, see Culture  
 defined, 12  
 disruptions, implications for resilience, see  
 Disruptions  
 factors, 239  
 measuring resilience, see Measuring  
 resilience  
 multidisciplinary challenge  
 phases, see Phases of resilience  
 protection vs. resilience, see Protection  
 resilience and resilience engineering  
 resilience architecting, see Architecting  
 resilience architectural hierarchy, 184–185  
 resilience engineering, xvii–xviii  
 signals of reduced resilience, 207
- Retaliation* heuristic, 175
- Reviews  
 defect review levels, 191  
 design level reviews, 191–192  
 detail reviews, 193  
 independent reviews, see Independent  
 reviews  
 system level reviews, 191  
 three-tiered view of technical reviews,  
 190–193
- Rewards and Incentives, 109
- Risk  
 acceptable risk philosophy, 59  
 as a consideration in resilience, 180–182  
 deficient on King’s Cross, 76  
 deficient on Seveso, 74  
 deficient on Windscale, 74–75  
 effect on resilience, 242

- Risk (*Continued*)  
 implementing in high-consequence or high-risk systems, see Implementation  
 limited visibility, 189  
 Massachusetts Institute of Technology (MIT) risk model, see Measuring resilience  
 operational risk management, 124  
 position within resilience architecture, 15  
 probabilistic risk analysis (PRA), see Measuring resilience  
*risk aggregation* heuristic, 181–182  
*Risk culture* heuristic, 182. See also Culture  
 risk denial paradigm, 41, 101–102  
 risk-based costing, see Cost  
 Royal Dutch/Shell case, 113  
 Rules, see Humans
- Safety, 31–33  
 as a metric, 204  
 industrial safety, 32  
 organizational safety, 32  
 system safety, 32  
 safety as a technical capability, 142–144
- Safety analysis paradigm, 100  
 Schedule management, 134  
 Scottish Railways Study, 8, 201  
 Second engineer method, Metrolink 111, 268  
 Self-discovery, the new model, 110–112  
 Sensitivity to operations and a reporting culture, 93–94
- Service quality  
 as a metric, 204
- Simplicity* heuristic, 170
- Seveso  
 case history, 73–74  
 resilience aspects, 75
- Sharp edge of the system, 88, 127  
 Signal gap theory, Metrolink 111, 262
- Sioux City  
 case history, 78–79  
 FAA propulsion decision, 215  
 graceful degradation heuristic, 172  
 resilience aspects, 78
- Small problem focus* heuristic, 181
- Socioecological systems, 20, 168
- Socratic teaching approach, 107
- Software  
 adaptability in software, see Adaptability  
 software as a technical capability, 146
- SpaceShipOne, 96
- STAMP (Systems-Theoretic Accident Modeling and Processes), 131
- Standard processes, 108  
 Statistical prediction, 201–203  
 Survival, 12–13, 165  
 Supplier Management, 136
- System  
 architecture of a system, 5. See also Architecture and Architecting  
 concept of the system, 3, 16  
 infrastructure as a system, 4. See also Infrastructure  
 Metrolink 111 system, 263–265  
 system types  
 complex adaptive systems (CASs), see Complex adaptive systems (CASs)  
 human-intensive, see Human-intensive systems  
 infrastructure, see Infrastructure systems  
 network-based, see Infrastructure  
 product-centered infrastructure, see Product-centered infrastructure systems  
 process, see Process systems  
 socioecological, see Socioecological systems  
 systems of systems, see Systems of systems and Federation of systems  
 technological, see Technological systems  
 technological with human interfaces, see Technological systems
- System safety, see Safety
- Systems approach, 29–31  
 approach of this book, ix  
 boundary, identification of system, 29, 39  
 elements, identification of system, 29  
 emergent characteristics, identification of system, 29  
 environment, identification of system, 29. See also Environment  
 function of each element, identification of, 29  
 grouping of elements, 29  
 inadequacy of analytic approaches within, 26  
 interaction among the elements, analysis of, 29  
 subdivision of elements into smaller elements, 29  
 synthesis of the system, 29  
 verification and validation of the system, 29
- Systems engineering, xviii  
 Systems engineering and integration team (SEIT), 135, 155
- Systems view, 116
- Systems of systems  
 as the system resilience infrastructure, 240  
 defined, 21–22

- infrastructure as a system of systems, see Infrastructure
  - managerial responsibilities, 124
  - Metrolink system of systems, 264
  - operational view, 152
  - Swiss cheese model, 47–48, 65, 148
- Tacoma Narrows Bridge
- case history, 79
  - disruption of input, Type A, 6, 28
  - example of Titanic Effect, 113
  - expertise factor, 17
  - hardware agent, 44
  - limited visibility factor, 189
  - resilience aspects, 80
  - unpredictability of disruption, 45, 51
- Teams approach, 107
- Technical management, 148
- Technological systems, 16–18
- technological systems with human interfaces, 19
- Technology management, 144
- technology readiness levels (TRLs), 141
- Texas City-1947
- case history, 59–60
  - resilience aspects, 60
  - deficient regulatory process, 135
- Texas City-2005
- case history, 60
  - culture aspects, 109, 234
  - resilience aspects, 61
- The Infrastructure Security Partnership (TISP), 157
- Third world application, 246
- Three Mile Island, 149
- case history, 66–67
  - resilience aspects, 67
- Tight and loose coupling, 14, 21, 48
- loose coupling* heuristic, 171
- Tight coupling, see Tight and loose coupling
- Titanic effect, 69, 96–97, 113
- Tolerance, 56, 123, 151
- as an attribute of adaptability, 171–175
  - deficient on Metrolink 111, 266
  - effect on resilience, 242
- Traditional paradigm change paradigm, 104
- Training
- approach for cultural change, 106
  - for humans on the “sharp edge,” 127
- TWA 800
- case history, 68–69
  - FAA fuel tank vapor decision, 214
  - resilience aspects, 69
- Twin towers attack, 36, 41
- Unpredicted disruptions, see Predicted vs. unpredictable disruptions
- Union Carbide factor, 50
- Union Pacific
- node of the Metrolink system, 264
- United Flight 93, 1
- US Airways 1549
- case history, 88–89
  - resilience aspects, 88
  - worst case scenario, 167
- Validation, 142. See also Systems approach
- Van Allen radiation belt, 51
- ValuJet
- boundary aspects, 27, 53, 240
  - case history, 80–81
  - deficient maintenance, 174, 205
  - requirements in breadth, 141
  - resilience aspects, 81
  - infrastructure disconnects, 23, 176
  - similarities to Concorde, 84
- Veolia Transportation,
- node of the Metrolink system, 263–264
- Verification, 141. See also Systems approach
- Deficient on Challenger, 58
- Video cameras, Metrolink 111, 270
- View, operational, see Infrastructure
- Windscale
- case history, 74–75
  - resilience aspects, 75
- Work environment, 135
- Xerox case, 113









