About the Author

Herbert Hecht is vice chairman of the Board of SoHaR Incorporated, an R&D and consulting company for high dependability systems. (The name of the company is a contraction of software and hardware reliability.) In addition to his managerial duties, he supervises technical work in hardware and software reliability analysis, sneak circuit analysis, and safety analysis.

His expertise has caused him to be appointed to many governmental and academic review bodies for safety and reliability, such as the National Research Council’s Committee on Engineering Challenges to the Long-Term Operation of the International Space Station (a congressionally mandated committee), 1998–2000, and the Nuclear Regulatory Commission’s Expert Panel on Digital System Research, 1999. He has participated in the NASA Ames Workshop for Design for Safety and in safety investigations at the NASA Jet Propulsion Laboratory.

Prior to founding SoHaR, Dr. Hecht was employed at The Aerospace Corporation, El Segundo, California (1962–1977), leaving as director of Digital Systems for Advanced Programs. One of his assignments was the development of the Ascent Guidance Monitoring System for the Gemini Launch Vehicle (GLV), and in that role he participated in the first two launches of the GLV. Earlier, he was employed at the Sperry Corporation as department head for Helicopter Flight Controls. He developed and managed the development of navigation and flight control systems that required extremely high dependability.

Dr. Hecht’s professional activities include a term on the Board of Governors of the IEEE Computer Society, service as Visitor in Computer Engineering for ABET, and membership in standards working groups of the IEEE, the AIAA, and the ISA. He has more than 100 papers in refereed journals or
conference proceedings and holds 12 patents in the field of highly reliable control systems. He is licensed as a professional engineer in control systems engineering by the state of California.

Dr. Hecht received a bachelor of electrical engineering degree from City College, New York, and a master’s degree in the same subject from Polytechnic Institute of Brooklyn (now part of Polytechnic University). In 1967 he received a Ph.D. in engineering from the University of California at Los Angeles, with a dissertation on economics of reliability for space launch vehicles.
Index

Action items, 155
Activity blocks, 138
Adaptive changes, 147
Aircraft electronics bay, 210–15
  channel processing failure rate, 214
  failure rate contributors, 213
  partial improvement of function, 213–15
  power distribution, 210
  power supply failure probabilities, 211
  primary power supply, 210–11
  safety critical loads, 211–13
  timing and synchronization (T&S) components, 214
See also Applications
Alternates
  active, 97–98
  diverse, 95–96
  dormant, 97–98
  identical, 95–96

The American National Standard
Recommended Practice for
Software Reliability, 112

Analytical approaches, 37–61
  classes, 37
  failure modes and, 38–52
  fault tree analysis (FTA), 56–61
  sneak circuit analysis (SCA), 52–56
  summary, 61
Analytical redundancy, 105–6
  advantages, 106
  defined, 105
  example, 105–6
  uses, 105–6

Applications, 199–219
  aircraft electronics bay, 210–15
  overview, 199–200
  power supply, 200–210
  spacecraft attitude determination, 215–18
  summary, 219
Audits, 153
Aviation accidents, 29–31
  American Airlines flight 1420, 29
  Hageland Aviation, 30–31
  TWA flight 800, 30
See also Failure(s)

Base failure rates, 8
Behaviors, 127
Breadboard test, 73
Built-in test (BIT), 55, 83–84
  characteristics, 83
  equipment, 83
See also In-service testing
Changes
- adaptive, 147
- perfective, 147
- system reliability effects, 147–48

Chernobyl, 27–29
- accident cause, 28
- defined, 27
- operator actions, 28
- postaccident safety measures, 28–29
- reactor features, 27
  See also Failure(s)

Common power supplies, 201–6
- availability, 203
- defined, 201–2
- illustrated, 202
- isolating diodes, 202
- RBD for, 203
  See also Power supplies

Communication satellites
- communication payload, 196
- failure probabilities, 196
- life factors, 195
- replacement of, 195–97
- replacement scheduling, 195

Component prototype test, 74

Computer-based tools, 46

Concept phase, 137
- answers, 142
- reliability issues, 141–42
- start of, 141
  See also Life cycle

Condition tables, 121, 122

Configuration(s)
- control, 158
- management, 141
- orthogonal gyros, 215–16
- quadruple voting, 102

Control charts, 159–60
- defined, 159–60
- use of, 160
- in visualization, 160
  See also Quality assurance

Cost
- elements, estimation, 174–77
- expected, of failure, 176
- of failure, 167–82
- fault tolerance, 131
- generic, of reliability model, 177–81
- increment for reliability, 168
- relations for reliability improvement, 169
- testing, 63, 152
- total, 186, 187
- total user curve, 170
- trade-offs, 183–98

Could not duplicate (CND), 72, 145

Coverage
- accounting for, 94–95
- defined, 94
- imperfect, 94–95
- imperfect, effect of, 95

Dedicated power supplies, 206–8
- box replacement, 208
- channel independence, 207
- channel unavailability, 207
- defined, 206
- illustrated, 207
- MTBF of, 209–10
  See also Power supplies

Design and evaluation tasks, 150

Design margins, 66–70
- increased, 174–75, 181
- normalized, 67
- probability of failure vs., 67

Detector threshold, 68
- distributions, 69
- mean, 68

Development phase
- end of, 144
- failure prevention and, 142
- reliability and, 137
- reliability issues in, 142–44
- requirements release, 141
- spiral model for, 140
- transition to, 141
- waterfall model for, 139
  See also Life cycle

Discrete parameter model, 14–15
- availability computed from, 15
- defined, 14
- probability calculation, 15

Discrimination ratio, 65

Dual redundancy, 91–98
- active vs. dormant alternates, 97–98
- dynamic, 91–95
- identical vs. diverse alternates, 95–96
- static, 91–95
  See also Redundancy

Dynamic redundancy, 91–95
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>defined</td>
<td>91</td>
</tr>
<tr>
<td>illustrated</td>
<td>92</td>
</tr>
<tr>
<td>requirement</td>
<td>92–93</td>
</tr>
<tr>
<td>software application</td>
<td>129, 131</td>
</tr>
<tr>
<td>See also Redundancy</td>
<td></td>
</tr>
<tr>
<td>Electronic parts tolerance analysis</td>
<td>151</td>
</tr>
<tr>
<td>Embedded software</td>
<td>109</td>
</tr>
<tr>
<td>End-of-period uniform payments</td>
<td>173</td>
</tr>
<tr>
<td>Engineering change proposal (ECP)</td>
<td>139</td>
</tr>
<tr>
<td>Environmental stress screening (ESS)</td>
<td>152</td>
</tr>
<tr>
<td>Error detecting and correcting code (EDAC)</td>
<td>82</td>
</tr>
<tr>
<td>Error detecting codes (EDC)</td>
<td>82–83</td>
</tr>
<tr>
<td>arithmetic operations for</td>
<td>105</td>
</tr>
<tr>
<td>characteristics</td>
<td>83</td>
</tr>
<tr>
<td>in digital operations</td>
<td>93</td>
</tr>
<tr>
<td>using</td>
<td>82</td>
</tr>
<tr>
<td>Error detection</td>
<td>93–94</td>
</tr>
<tr>
<td>Expenditures</td>
<td></td>
</tr>
<tr>
<td>administrative obstacles and</td>
<td>171</td>
</tr>
<tr>
<td>benefits and</td>
<td>171, 172, 173, 174</td>
</tr>
<tr>
<td>financial modeling</td>
<td>173</td>
</tr>
<tr>
<td>periodic uniform</td>
<td>173</td>
</tr>
<tr>
<td>single</td>
<td>171</td>
</tr>
<tr>
<td>time considerations</td>
<td>170–74</td>
</tr>
<tr>
<td>uncertain benefits and</td>
<td>171</td>
</tr>
<tr>
<td>See also Cost</td>
<td></td>
</tr>
<tr>
<td>Exponential distribution</td>
<td>5–8</td>
</tr>
<tr>
<td>defined</td>
<td>6</td>
</tr>
<tr>
<td>illustrated</td>
<td>6</td>
</tr>
<tr>
<td>Extreme programming</td>
<td>141</td>
</tr>
<tr>
<td>Failure analysis and corrective action</td>
<td></td>
</tr>
<tr>
<td>procedure (FRACAS)</td>
<td>64</td>
</tr>
<tr>
<td>good</td>
<td>70</td>
</tr>
<tr>
<td>key entries</td>
<td>70–72</td>
</tr>
<tr>
<td>Failure modes, effects and criticality</td>
<td></td>
</tr>
<tr>
<td>analysis (FMECA)</td>
<td>38</td>
</tr>
<tr>
<td>Failure modes and effects analysis (FMEA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>38–52</td>
</tr>
<tr>
<td>alternative approaches</td>
<td>46–49</td>
</tr>
<tr>
<td>applications</td>
<td>38</td>
</tr>
<tr>
<td>concepts</td>
<td>38–39</td>
</tr>
<tr>
<td>documentation</td>
<td>39</td>
</tr>
<tr>
<td>documents generated from</td>
<td>50</td>
</tr>
<tr>
<td>for electronic artillery fuze</td>
<td>48</td>
</tr>
<tr>
<td>failure probability estimates</td>
<td>42</td>
</tr>
<tr>
<td>flight phase failure effects</td>
<td>45</td>
</tr>
<tr>
<td>flight phase failure effects summary</td>
<td>44</td>
</tr>
<tr>
<td>functional approach</td>
<td>47, 48</td>
</tr>
<tr>
<td>model-based development and</td>
<td>49</td>
</tr>
<tr>
<td>parts approach</td>
<td>48</td>
</tr>
<tr>
<td>as plan for action</td>
<td>49–52</td>
</tr>
<tr>
<td>in process industry</td>
<td>38</td>
</tr>
<tr>
<td>for project support activities</td>
<td>49–50</td>
</tr>
<tr>
<td>of protective components</td>
<td>204</td>
</tr>
<tr>
<td>report organization</td>
<td>41–45</td>
</tr>
<tr>
<td>report table of contents</td>
<td>43</td>
</tr>
<tr>
<td>systematic deficiency</td>
<td>145</td>
</tr>
<tr>
<td>top-down presentation</td>
<td>44</td>
</tr>
<tr>
<td>updates</td>
<td>140</td>
</tr>
<tr>
<td>worksheet example</td>
<td>39</td>
</tr>
<tr>
<td>worksheets</td>
<td>38–52</td>
</tr>
<tr>
<td>Failure not verified (FNV)</td>
<td>72</td>
</tr>
<tr>
<td>Failure prevention</td>
<td>1</td>
</tr>
<tr>
<td>analytical approaches to</td>
<td>37–61</td>
</tr>
<tr>
<td>contributions to</td>
<td>163</td>
</tr>
<tr>
<td>development phase and</td>
<td>142</td>
</tr>
<tr>
<td>in life cycle</td>
<td>137–64</td>
</tr>
<tr>
<td>practices</td>
<td>120–29</td>
</tr>
<tr>
<td>requirements</td>
<td>120–22</td>
</tr>
<tr>
<td>test</td>
<td>122–26</td>
</tr>
<tr>
<td>testing for</td>
<td>63–85</td>
</tr>
<tr>
<td>UML-based software development</td>
<td>126–29</td>
</tr>
<tr>
<td>Failure probability</td>
<td>1, 65, 66, 176</td>
</tr>
<tr>
<td>aircraft electronics power supply</td>
<td>211</td>
</tr>
<tr>
<td>estimate uncertainties</td>
<td>176</td>
</tr>
<tr>
<td>nonorthogonal gyros</td>
<td>217</td>
</tr>
<tr>
<td>orthogonal gyros</td>
<td>216</td>
</tr>
<tr>
<td>reduction estimation</td>
<td>175</td>
</tr>
<tr>
<td>reduction in</td>
<td>179</td>
</tr>
<tr>
<td>for satellite subsystems</td>
<td>196</td>
</tr>
<tr>
<td>Failure processing template</td>
<td>146</td>
</tr>
<tr>
<td>Failure rate(s)</td>
<td></td>
</tr>
<tr>
<td>base</td>
<td>8</td>
</tr>
<tr>
<td>channel processing</td>
<td>214</td>
</tr>
<tr>
<td>denominator</td>
<td>16–18</td>
</tr>
<tr>
<td>expression</td>
<td>16–18</td>
</tr>
<tr>
<td>flight control electronics</td>
<td>213</td>
</tr>
<tr>
<td>improved flight control electronics</td>
<td>214</td>
</tr>
<tr>
<td>numerator</td>
<td>16</td>
</tr>
<tr>
<td>published</td>
<td>8</td>
</tr>
<tr>
<td>Failure Review Board (FRB)</td>
<td>72</td>
</tr>
<tr>
<td>Failure(s)</td>
<td></td>
</tr>
<tr>
<td>analysis</td>
<td>161–62</td>
</tr>
<tr>
<td>aviation</td>
<td>29–31</td>
</tr>
</tbody>
</table>
Failure(s) (continued)
- in calendar time, 17
- causes, 9
- Chernobyl, 27–29
- common threads, 32–34
- cost, 167–82
- developer’s view, 16
- exposure to, 16
- histories, 143
- inevitability and, 21–22
- Mars spacecraft, 23–26
- nonchangeable, 147
- nonrandom, 96
- in operating time, 17
- organizational causes, 21–34
- probable cause summary, 33
- rare conditions for, 119
- rates, 88
- reporting, units of time, 18
- reporting system, 72
- software, 109–14
- space shuttle Columbia, 26–27
- telecommunications, 31–32
- thoroughly documented, 22–32

Failure/value (F/V) ratio, 180

Faults
- density, 112, 113
- exposure ratio, 113
- identification, 113
- interval for counting, 113
- removed, as found, 132

Fault tolerance, 129–32
- cost, 131
- dynamic, 131
- RBD for, 132
- static, 131

Fault tree analysis (FTA), 56–61
- application, 57
- basics, 57–58
- defined, 56–57
- example, 58–61
- as hierarchical procedure, 57–58
- missile detonation circuit, 58, 59
- symbols, 57
See also Analytical approaches

Field failures
- causes, 8–12
- event classifications, 81
- investigations, 81–82

not verified (FFNV), 145
See also Failure(s)

Field test set (FTS), 82, 84
- time trends analysis, 84
- use of, 84
See also In-service testing

First article acceptance test, 75

Fully automated implementation, 191, 192

Functional allocation, 150

General purpose computer (GPC), 102
Government Industry Data Exchange Program (GIDEP), 159, 162

Gyros, 215–17
- nonorthogonal orientation, 217–18
- orthogonal configurations, 215–17

In-house monitoring, 159–62
- awareness of technical information, 162
- failure reporting/analysis, 161–62
- quality assurance, 159–61
See also Monitoring

In-service testing, 82–84
- built-in test, 83–84
- EDCs, 82–83
- FTS, 84

Interest groups, 3–4

k-out-of-n redundancy, 102–5
- capabilities, 104
- example, 103
- selection mechanism, 104
- symbols, 103

Life cycle
- activity blocks, 138
- activity elements, 137
- development phase, 137, 139
- failure cause introduction and, 163
- failure prevention in, 137–64
- format, 138–41
- milestones, 138
- phases, 137
- phases, reliability issues and, 141–48
- reliability and, 137
- spiral model, 139–40
- terminology, 138
- waterfall charts, 138, 139

Littlewood-Verall (L-V) model, 132

Maintenance
- budget, 193
effectiveness, increasing, 192–95
records, 193
repair actions, 193
Mars Climate Orbiter (MCO), 23
budget, 25
failure, 24
Mars Polar Lander (MPL), 23
budget, 25
failure cause, 23–24
sequence of operations, 24
See also Failure(s)
Mars spacecraft failures, 23–26
Mean-time-between-failures (MTBF), 7
assumptions on unavailability, 209
claim, 65
of dedicated power supply, 209–10
demonstrated, 64
ratio, 65
Mean-time-to-failure (MTTF), 7
Mean-time-to-repair (MTTR), 14
Medford switching center, 31
Mercury-Redstone launch, 52
Methods, 126–27
Milestones, 138
Model-based development, 49
Monitoring, 157–62
critical items, 157–62
in-house, 159–62
purchased items, 158–59
for reliability attainment, 159–62
Next highest level (NHL), 40, 41
N-modular redundancy (NMR), 99
Nonchangeable failures, 147
Nonoperating Reliability Databook, 98
Nonorthogonal gyros
failure probability, 217
orientation, 217–18
reference axes, 217
See also Gyros
Normalized margins, 67
O&M phase, 137
FRACAS focus, 163
problem reports, 144–45
reliability issues in, 144–48
See also Life cycle
Operational capability (IOC), 75
Operational evaluation, 75–76
Optimum reliability, 167–70
concept, 167
starting point, 168
Organization, this book, 2–3
Organizational causes, 21–34
Orthogonal gyros
configurations, 215–16
failure probability, 216
reference axes, 216
See also Gyros
Pair-and-pair redundancy, 102
Pair-and-space redundancy, 101–2
benefits, 101
defined, 101
illustrated, 102
Parameter estimation, 8–9
Pareto distribution, 47, 77
Partial redundancy, 178
Partitioned redundancy, 90
Partitioning, 90–91
effect on failure probability, 91
Stratus, 91
Parts evaluation, 72–73
Perfetctive changes, 147
Plant simulation, 123–24
Poisson distribution, 6
Power outages
commercial, 185
duration plot, 186
fully automated alternative, 191, 192
notification function, 190
semasautomated alternative, 191–92
tolerating, 187
Power supplies, 200–210
alternative characteristics, 209
alternatives, 201–8
alternatives evaluation, 208–10
box replacement probability, 203–4
common, 201–6
dedicated, 206–8
location, 200
magnetic circuit breakers, 206
power diode, 205
protective components, 204, 205
selection framework, 200–201
See also Applications
Prism program, 9
Probability of failure, 1, 65, 66, 89
attitude determination, 218
calculation, 69
Probability of failure (continued)
difference distribution and, 70
due to test case, 126
for low values of \( M \), 68
normalized margin vs., 67
partitioning effect on, 91
of TMR and simplex systems, 100
See also Failure(s)

Problem reports, 144–45
could not duplicate (CND), 145
defined, 144
field failure not verified (FFNV), 145

Process control deviations, 158–59
Process improvement, 174, 181
Production reliability acceptance tests (PRAT), 152

Quadruple redundancy, 106
Quadruple voting configurations, 102
Qualification test, 74–75
data evaluation issues, 75
defined, 74
See also Tests

Quality assurance, 159–61
control chart, 159–60
statistical parameter presentation, 160

Quality of service (QoS), 183

Quantitative allocation, 150

Rapid prototyping, 141

Rare events (REs), 117
causes, 117
multiple, 117, 124, 126
probability of, 125
RR ratio, 124

Real-time software, 109

Receive HB method, 128
counter method, 128
failure mode, 128
FMEA worksheet for, 129
HB failure, 129
use case diagram, 128

Redundancy, 175, 182
added resource for, 178
analytical, 105–6
architecture comparison, 107
at component level, 87–91
dual, 91–98
dynamic, 91–95
higher-order configurations, 102–5
\( k \)-out-of-\( n \), 102–5
pair-and-pair, 102
pair-and-spare, 101–2
partitioned, 90
with power switching, 97
quadruple, 106
risk for, 175
static, 91–95
summary, 106
techniques, 87–107
temporal, 105
triple, 98–102
triple modular (TMR), 92, 99–101

Reliability
aim, 1
of aircraft electronics bay, 210–15
assessment, 70
change effects on, 147–48
concept phase and, 141–42
cost increment, 168
data, 9
defined, 6
demonstration, 64–66
development phase and, 137, 142–44
engineering, 5–19
of explosive device components, 8
initial planning, 144
life cycle and, 137
nonmonetary resources and, 34
of \( n \)-redundant component, 177
O&M phase and, 144–48
optimum, 167–70
partial, 178
qualification test (RQT), 152
relevance of postdevelopment tests, 76–82
relevance of tests during development,
70–76
requirements, 151
resources, 34
software, 109–33
testing, 64
trends for redundant configurations,
88, 89
Reliability allocation, 150–51
effort allocated to, 151
functional, 150
quantitative, 150

Reliability block diagrams (RBD), 9–12
common power supplies, 203
conventional, 12
Space Shuttle Avionics (SSA) software, 116
Space shuttle Columbia, 26–27
  investigation, 26
  organizational causes, 26–27
  See also Failure(s)
Spiral model, 139–40
  defined, 139
  for development phase, 140
  See also Life cycle
State transition diagrams
  defined, 13
  illustrated, 14
  uses, 14
State transition methods, 12–16
Static redundancy, 91–95
  defined, 91
  illustrated, 92
  for mechanical elements, 92
  software application, 129, 131
  See also Redundancy
System failure effects summary, 44
System integration test, 74
System reliability. See Reliability
Telecommunications, 31–32
  Medford switching facility, 31
  Salt Lake City central office, 31–32
Temporal redundancy, 105
Testing, 63–85, 152
  by attributes, 70
  code-based, 122
  for contractual purposes, 64
  cost, 63, 152
  for design margins, 63
  early, 63
  in-service, 82–84
  random, 122
  reliability, 64
  requirements-based, 122
  software, 114–20
  summary, 85
  by variables, 70
Tests
  breadboard, 73
  component prototype, 74
  during development, 70–76
  environmental stress screening (ESS), 152
  first article acceptance, 75
  plan, 71
  postdevelopment, 76–82
  procedure, 71
  production reliability acceptance (PRAT), 152
  purpose, 73
  qualification, 74–75
  reliability development/growth (RDGT), 152
  reliability qualification (RQT), 152
  reliability relevance of, 70–82
  report, 71
  results, quantitative recording of, 73
  routine acceptance, 76–78
  screening, 78–81
  selection, 63
  specification, 71
  system integration, 74
  typical, 73
Time to restore service (TTRS), 18
  in availability calculations, 18
  defined, 18
  Triple modular redundancy (TMR), 92, 99–101
    applications, 100
    defined, 99
    failure probability, 100
    with voting, 99
    See also Redundancy
  Triple redundancy, 98–102
    pair-and-space, 101–2
    TMR, 99–101
    See also Redundancy
  UML-based software development, 126–29
    tools, 126
    use case diagram, 127–28
  Uniform Modeling Language (UML), 49
  Uninterruptible power supply (UPS), 184
  Use case diagrams, 127–28
    active/standby, 127
    defined, 127
    receive HB, 128
  Waterfall charts, 138–39
    defined, 138
    for development phase, 139
    See also Life cycle
  Work breakdown structure (WBS), 148