Annex C

Additional Resources

This collection of additional resources lists the sources that were used during the development of this book and provides pointers to additional resources that may be of interest to the reader. It is organized in three parts: (1) standards, policy, and regulations; (2) publications; and (3) online resources.

C.1 Standards and Regulations

This section lists contemporary and historical standards related to various aspects of information assurance. Given that most national and international standards are reaffirmed, updated, or withdrawn on a three- to five-year cycle, for implementation or assessment purposes, one should always verify that one has the current approved version.

American National Standards Institute (ANSI)

1. ANSI X3.92-1981, Data Encryption Algorithm (DEA), (reaffirmed 1987).
2. ANSI X3.105-1983, Information Systems: Data Link Encryption, (reaffirmed 1996).
3. ANSI X3.106-1983, Information Systems: Data Encryption Algorithm — Modes of Operation, (reaffirmed 1996).
4. ANSI X9.8.1-1995, Banking — Personal Identification Number Management and Security — Part 1: PIN Protection Principles and Techniques.
5. ANSI X9.8.2-1995, Banking — Personal Identification Number Management and Security — Part 2: Approved Algorithms for PIN Encipherment.
6. ANSI X9.9-1986, Financial Institution Message Authentication (Wholesale), (reaffirmed 1994).
7. ANSI X9.17-1995, Financial Institution Key Management (Wholesale).
8. ANSI X9.19-1996, Financial Institution Retail Message Authentication.
9. ANSI X9.23-1995, Financial Institution Encryption of Wholesale Financial Messages.
10. ANSI X9.24-1992, Financial Services — Retail Management.

11. ANSI X9.26-1990, Financial Institution Sign-On Authentication for Wholesale Financial Systems, (reaffirmed 1996).
12. ANSI X9.28-1991, Financial Services — Financial Institution Multiple Center Key Management (Wholesale).
13. ANSI X9.30.1-1995, Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry — Part 1: Digital Signature Algorithms (DSA).
14. ANSI X9.30.2-1995, Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry — Part 2.
15. ANSI/NIST-CSL 1-1993, Information Systems — Data Format for the Interchange of Fingerprint Information.
16. ANSI/IAI 1-1988, Forensic Identification — Automated Fingerprint Identification Systems — Benchmark Tests of Relative Performance.
17. ANSI/IAI 2-1988, Forensic Identification — Automated Fingerprint Identification Systems — Glossary of Terms and Acronyms.

*Canadian**

18. CE-1001-STD Rev. 1, Standard for Software Engineering of Safety Critical Software, CANDU Computer Systems Engineering Centre for Excellence, January 1995.
19. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Canadian System Security Centre, version 3.0e, 1993.

*European***

20. BS5760 Part 8: Guide to the Assessment of Reliability of Systems Containing Software, British Standards Institution (BSI), October 1998.
21. BS 7799-1:1999, Information Security Management. Code of Practice for Information Security Management, British Standards Institute.
22. BS 7799-2:1999, Information Security Management. Specification for Information Security Management Systems, British Standards Institute.
23. BSI/DISC PD3002:1998, Guide to BS 7799 Risk Assessment and Risk Management, British Standards Institute.
24. EN 50128:1997, Railway Applications: Software for Railway Control and Protection Systems, the European Committee for Electrotechnical Standardization (CENELEC).
25. Information Technology Security Evaluation Criteria (ITSEC), Commission of the European Communities, Provisional Harmonized Criteria, version 1.2, June 1991.
26. Information Technology Security Evaluation Manual (ITSEM), Commission of the European Communities, 1992.
27. Secure Information Processing versus the Concept of Product Evaluation, Technical Report ECMA TR/64, European Computer Manufacturer's Association (ECMA), December 1993.
28. Space Product Assurance: Policy and Principles, European Space Agency, ECSS-Q-00A, April 19, 1996.

---

* Engineering Standards, Nuclear Operations Services and Support, Ontario Power Generation, Inc., MS: H10 F5, 700 University, Toronto, Ontario, Canada M5G 1X6.

** BSI - www.bsi.org.uk.
CENELEC - www.cenelec.be.
ESA - www.estec.esa.nl.
ITSEC - www.itsec.gov.uk.

29. Space Product Assurance: Quality Assurance, European Space Agency, ECSS-Q-20A, April 19, 1996.
30. Space Product Assurance: Dependability, European Space Agency, ECSS-Q-30A, April 19, 1996.
31. Space Product Assurance: Safety, European Space Agency, ECSS-Q-40A, April 19, 1996.
32. Space Product Assurance: Software Product Assurance, European Space Agency, ECSS-Q-80A, April 19, 1996.
33. Space Product Assurance: Electrical, Electronic, and Electromechanical (EEE) Components, European Space Agency, ECSS-Q-60A, April 19, 1996.
34. Space Product Assurance: Materials, Mechanical Parts and Processes, European Space Agency, ECSS-Q-70A, April 19, 1996.
35. Space Product Assurance: Programme Management, European Space Agency, ECSS-M-00, April 19, 1996.
36. Space Product Assurance: Guidelines for Software Dependability and Safety Techniques, ECSS-Q-80-3, draft, January 2000.
37. Space Product Assurance: Safety Management, European Space Agency, ECSS-Q-80-4, draft, January 2000.

*Institution of Electrical Engineers (IEE)**

38. SEMSPLC Guidelines, Safety-Related Application Software for Programmable Logic Controllers, IEE Technical Guidelines 8:1996.

*Institute of Electrical and Electronics Engineers (IEEE)***

39. IEEE Std. 802.10-1998, Standard for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security.
40. IEEE Std. 802.10a-1999, supplement a, Interoperable LAN/MAN Security: Architecture framework.
41. IEEE Std. 802.10c-1998, supplement c, Interoperable LAN/MAN Security: Key Management.
42. ANSI/IEEE Std. 982.1-1989, Standard Dictionary of Measures to Produce Reliable Software.
43. ANSI/IEEE Std. 982.2-1989, Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software.
44. IEEE Std. 610.12-1990, Glossary of Software Engineering Terms.
45. IEEE Std. 1363-2000, Standard Specifications for Public Key Cryptography.
46. IEEE Std. 1402-2000, Guide for Electric Power Substations Physical and Electronic Security.
47. IEEE Std. 1490-1998, Guide to the Project Management Body of Knowledge, Adoption of Project Management Institute standard.
48. IEEE P1540/D10.0, Standard for Lifecycle Processes — Risk Management, December 2000.
49. IEEE P2002, Recommended Practice for Information Technology — Internet Security Practices, (draft) January 2000.

* IEE Standards are available from: IEE, P.O. Box 96, Stevenage, Herts SG1 25D, U.K.

** IEEE Standards are available from: http://standards.ieee.org.

*International**

50. CCITT Recommendation X.509, version 3, The Directory — Authentication Framework, Consultation Committee International Telephone and Telegraph, June 1996.
51. CCITT Recommendation X.800, Security Architecture for Open Systems Interconnection for CCITT Applications, Consultation Committee International Telephone and Telegraph, 1991.
52. Common Criteria for Information Technology (IT) Security Evaluation, version 2.0, Common Criteria Editing Board (CCEB), May 1998.
53. Development Guidelines for Vehicle Based Software, The Motor Industry Software Reliability Association (MISRA™), November 1994.
54. Guidelines for the Security of Information Systems, Organization for Economic Cooperation and Development (OECD), November 1992.
55. IEC 300-2, Dependability Management — Part 2: Dependability Programme Elements and Tasks.
56. IEC 300-3-9(1995-12), Dependability Management — Part 3: Application Guide — Section 9: Risk Analysis of Technological Systems.
57. IEC 601-1-4(1996-06), Medical Electrical Equipment — Part 1: General Requirements for Safety — 4. Collateral Standard: Programmable Electrical Medical Systems.
58. ISO/IEC 15026(1998-04), Information Technology — System and Software Integrity Levels.
59. IEC 60812(1985), Analysis Techniques for System Reliability — Procedure for Failure Modes Effects Analysis (FMEA).
60. IEC 60880(1986-09), Software for Computers in Safety Systems of Nuclear Power Stations.
61. IEC 61025(1990), Fault Tree Analysis (FTA).
62. IEC 61078(1991), Analysis Techniques for Dependability — Reliability Block Diagram Method.
63. IEC 61508-1(1998-12), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 1: General Requirements.
64. IEC 61508-2(2000-05), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems.
65. IEC 61508-3(1998-12), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 3: Software Requirements.
66. IEC 61508-4(1998-12), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 4: Definitions and Abbreviations of Terms.
67. IEC 61508-5(1998-12), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 5: Examples of Methods for the Determination of Safety Integrity Levels.
68. IEC 61508-6(2000-04), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 6: Guidelines on the Application of Parts 2 and 3.
69. IEC 61508-7(2000-03), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems — Part 7: Overview of Techniques and Measures.
70. ISO/IEC 2382-2(1998-11) edition 2.0, Information Technology — Vocabulary — Part 8: Security.

---

* IEC - www.iec.ch.
MISRA - www.misra.org.uk.
OECD - www.oecd.org.
RTCA - RTCA, Inc., 1140 Connecticut Avenue NW, Suite 1020, Washington, D.C. 20036-4001, USA.
SAE - www.sae.org.

71. ISO/IEC 7498-2(1989-12), Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.
72. ISO/IEC 9579(2000-03), Information Technology — Remote Database Access for SQL with Security Enhancement.
73. ISO/IEC 9594-8(1995-09), Information Technology — Open Systems Interconnection — The Directory: Authentication Framework; 2nd ed.
74. ISO/IEC 9796(1991-09), Information Technology — Security Techniques — Digital Signature Scheme Giving Message Recovery.
75. ISO/IEC 9796-2(1997-09), Information Technology — Security Techniques — Digital Signature Scheme Giving Message Recovery, Part 2: Mechanism Using a Hash Function.
76. ISO/IEC 9796-3(2000-05), Information Technology — Security Techniques — Digital Signature Scheme Giving Message Recovery, Part 3: Discrete Logarithm Based Mechanisms.
77. ISO/IEC 9797(1994-04), Information Technology — Security Techniques — Data Integrity Mechanisms Using a Cryptographic Check Function Employing a Block Cipher Algorithm.
78. ISO/IEC 9797-1(1999-12), Information Technology — Security Techniques — Message Authentication Codes (MACs) — Part 1: Mechanism Using a Block Cipher.
79. ISO/IEC 9798-1(1997-08), Information Technology — Security Techniques — Entity Authentication Mechanisms — Part 1: General Model.
80. ISO/IEC 9798-2(1999-07), Information Technology — Security Techniques — Entity Authentication Mechanisms — Part 2: Mechanisms Using Symmetric Encipherment Algorithms.
81. ISO/IEC 9798-3(1998-10), Information Technology — Security Techniques — Entity Authentication Mechanisms — Part 3: Mechanisms Using Digital Signature Techniques.
82. ISO/IEC 9798-4(1999-12), Information Technology — Security Techniques — Entity Authentication Mechanisms — Part 4: Mechanisms Using a Cryptographic Check Function.
83. ISO/IEC 9798-5(1999-03), Information Technology — Security Techniques — Entity Authentication Mechanisms — Part 5: Mechanisms Using Zero Knowledge Techniques.
84. ISO/IEC 9979(1999-03), Information Technology — Security Techniques — Procedures for the Registration of Cryptographic Algorithms.
85. ISO/IEC 10116(1997-04), Information Technology — Security Techniques — Modes of Operation for an n-bit Block Cipher.
86. ISO/IEC 10118-1(2000-06), Information Technology — Security Techniques — Hash Functions — Part 1: General.
87. ISO/IEC 10118-2(1994-10), Information Technology — Security Techniques — Hash Functions — Part 2: Hash Functions Using an n-bit Block Cipher Algorithm.
88. ISO/IEC 10118-3(1998-06), Information Technology — Security Techniques — Hash Functions — Part 3: Dedicated Hash Functions.
89. ISO/IEC 10118-4(1998-06), Information Technology — Security Techniques — Hash Functions — Part 4: Hash Functions Using Modular Arithmetic.
90. ISO/IEC 10164-7(1992-05), Information Technology — Open Systems Interconnection — Systems Management: Security Alarm Reporting Function.
91. ISO/IEC 10164-8(1993-06), Information Technology — Open Systems Interconnection — Systems Management: Security Audit Trail Function.
92. ISO/IEC 10164-9(1995-12), Information Technology — Open Systems Interconnection — Systems Management: Objects and Attributes for Access Control.
93. ISO/IEC 10181-1(1996-08), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Overview.
94. ISO/IEC 10181-2(1996-05), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Authentication Framework.

95. ISO/IEC 10181-3(1996-09), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Access Control Framework.
96. ISO/IEC 10181-4(1997-04), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Non-Repudiation Framework.
97. ISO/IEC 10181-5(1996-09), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Confidentiality Framework.
98. ISO/IEC 10181-6(1996-09), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Integrity Framework.
99. ISO/IEC 10181-7(1996-08), Information Technology — Open Systems Interconnection — Security Framework for Open Systems: Security Audit and Alarm Framework.
100. ISO/IEC 10736(1995-04), Information Technology — Telecommunications and Information Exchange Between Systems — Transport Layer Security Protocol (TLS).
101. ISO/IEC 10745(1995-08), Information Technology — Open Systems Interconnection — Upper Layers Security Model.
102. ISO/IEC 11577(1995-05), Information Technology — Open Systems Interconnection — Network Layer Security Protocol (NLS).
103. ISO/IEC 11586-1(1996-06), Information Technology — Open Systems Interconnection — Generic Upper Layers Security: Overview, Models, and Notation.
104. ISO/IEC 11586-2(1996-06), Information Technology — Open Systems Interconnection — Generic Upper Layers Security: Security Exchange Service Element (SESE) service definition.
105. ISO/IEC 11586-3(1996-06), Information Technology — Open Systems Interconnection — Generic Upper Layers Security: Security Exchange Service Element (SESE) Protocol Specification.
106. ISO/IEC 11586-4(1996-06), Information Technology — Open Systems Interconnection — Generic Upper Layers Security: Protecting Transfer Syntax Specification.
107. ISO/IEC 11770-1(1997-01), Information Technology — Security Techniques — Key Management — Part 1: Framework.
108. ISO/IEC 11770-2(1996-04), Information Technology — Security Techniques — Key Management — Part 2: Mechanisms Using Symmetric Techniques.
109. ISO/IEC 11770-3(1999-11), Information Technology — Security Techniques — Key Management — Part 3: Mechanisms Using Asymmetric Techniques.
110. ISO/IEC 13335-1(1997-01), Information Technology — Guidelines for the Management of IT Security — Part 1: Concepts and Models for IT Security.
111. ISO/IEC 13335-2 (1998-01), Information Technology — Guidelines for the Management of IT Security — Part 2: Managing and Planning IT Security.
112. ISO/IEC 13335-3 (1998-06), Information Technology — Guidelines for the Management of IT Security — Part 3: Techniques for the Management of IT Security.
113. ISO/IEC 13335-4 (2000-3), Information Technology — Guidelines for the Management of IT Security — Part 4: Selection of Safeguards.
114. ISO/IEC 13888-1(1997-12), Information Technology — Security Techniques — Non-repudiation — Part 1: General.
115. ISO/IEC 13888-2(1998-04), Information Technology — Security Techniques — Non-repudiation — Part 2: Mechanisms Using Symmetric Techniques.
116. ISO/IEC 13888-3(1997-12), Information Technology — Security Techniques — Non-repudiation — Part 3: Mechanisms Using Asymmetric Techniques.
117. ISO/IEC 14888-1(1999-12), Information Technology — Security Techniques — Digital Signature with Appendix, Part 1: General.
118. ISO/IEC 14888-2(1999-12), Information Technology — Security Techniques — Digital Signature with Appendix, Part 2: Identity-Based Mechanisms.
119. ISO/IEC 14888-3(1999-12), Information Technology — Security Techniques — Digital Signature with Appendix, Part 3: Certificate-Based Mechanisms.

120. ISO/IEC 15408-1(1999-12), Information Technology — Security Techniques — Common Criteria for IT Security Evaluation (CCITSE) — Part 1: General Model.
121. ISO/IEC 15408-2(1999-12), Information Technology — Security Techniques — Common Criteria for IT Security Evaluation (CCITSE) — Part 2: Security Functional Requirements.
122. ISO/IEC 15408-3(1999-12), Information Technology — Security Techniques — Common Criteria for IT Security Evaluation (CCITSE) — Part 3: Security Assurance Requirements.
123. ISO/IEC 17799(2000-12), Information Technology — Code of Practice for Information Security Management.
124. JA 1002, Software Reliability Program Standard, Society of Automotive Engineers (SAE), 1998.
125. RTCA/DO-178B: Software Considerations in Airborne Systems and Equipment Certification, Requirements and Technical Concepts in Aviation, Inc., December 1, 1992.

*National Aeronautics and Space Administration (NASA)**

126. NASA-STD-8719.13A, Software Safety, NASA Technical Standard, September 15, 1997.
127. NASA GB-1740.13.96, Guidebook for Safety-Critical Software — Analysis and Development, NASA Glenn Research Center, Office of Safety and Mission Assurance, 1996.

North Atlantic Treaty Organization (NATO)

128. Commercial Off-the-Shelf (COTS) Software Acquisition Guidelines and COTS Policy Issues, Communications and Information Systems Agency, NATO, January 10, 1996, 1st revision.

*U.K. Ministry of Defence (MoD)***

129. DEF STAN 00-55: Requirements for Safety Related Software in Defence Equipment, Part 1: Requirements, U.K. Ministry of Defence (MoD), August 1, 1997.
130. DEF STAN 00-55: Requirements for Safety Related Software in Defence Equipment, Part 2: Guidance, U.K. Ministry of Defence (MoD), August 1, 1997.
131. DEF STAN 00-41/Issue 3, Reliability and Maintainability, MoD Guide to Practices and Procedures, U.K. Ministry of Defence (MoD), June 25, 1993.
132. DEF STAN 00-42/Issue 1, Reliability and Maintainability Assurance Guides, Part 2: Software, U.K. Ministry of Defence (MoD), September 1, 1997.
133. DEF STAN 00-58: HAZOP Studies on Systems Containing Programmable Electronics, Part 1: Requirements, U.K. Ministry of Defence (MoD), (interim) July 26, 1996.
134. DEF STAN 00-58: HAZOP Studies on Systems Containing Programmable Electronics, Part 2: Guidance, U.K. Ministry of Defence (MoD), (interim) July 26, 1996.

* NASA standards are available from: www.ivv.nasa.gov or www.gsfc.nasa.gov.
** MoD Standards are available from: www.mod.uk.

U.S. Department of Defense (DoD)*

135. CSC-STD-001-83, Trusted Computer System Evaluation Criteria (TCSEC), National Computer Security Center, U.S. Department of Defense, August 15, 1983.
136. CSC-STD-003-85, Guidance for Applying the Trusted Computer System Evaluation Criteria in Specific Environments, National Computer Security Center, U.S. Department of Defense, June 1985.
137. CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-83, National Computer Security Center, U.S. Department of Defense, 1985.
138. CSC-EPL-85/001, Final Evaluation Report of SCOMP (Secure Communications Processor) STOP Release 2.1, U.S. Department of Defense, September 23, 1985.
139. DDS-2600-6243-91, Compartmented Mode Workstation Evaluation Criteria, Defense Intelligence Agency (DIA), U.S. Department of Defense, version 1, 1991.
140. DOD 5200.28-M, ADP Computer Security Manual — Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, with 1st amendment, U.S. Department of Defense, June 25, 1979.
141. DOD-5200.28-STD, Trusted Computer System Evaluation (TCSEC), National Computer Security Center, U.S. Department of Defense, December 1985.
142. Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, 3rd ed., Joint Chiefs of Staff, U.S. Department of Defense, September 17, 1997.
143. MIL-STD-882D, Mishap Risk Management (System Safety), U.S. Department of Defense (DoD) Standard Practice, (draft) October 20, 1998.
144. NCSC-TG-005 version 1, Trusted Network Implementation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, U.S. Department of Defense, July 1987.
145. NCSC-TG-011 version 1, Trusted Network Interpretation (TNI), National Computer Security Center, U.S. Department of Defense, August 1, 1990.
146. NCSC-TG-021 version 1, Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, U.S. Department of Defense, April 1991.
147. NCSC-TG-025 version 2, A Guide to Understanding Data Remembrance in Automated Information Systems, National Computer Security Center, U.S. Department of Defense, September 1991.
148. Systems Security Engineering Capability Maturity Model (SSE-CMM), version 2.0, April 1, 1999.
149. SSE-CMM Appraisal Method, version 2.0, April 16, 1999.
150. PKI Roadmap for the U.S. Department of Defense, December 13, 1999.
151. X.509 Certificate Policy (CP) for the U.S. Department of Defense, version 5.0, December 13, 1999.
152. Information Assurance Technical Framework (IATF), National Security Agency IA Solutions Technical Directors, Release 3.0, September 2000.

U.S. National Institute of Standards and Technology (NIST)**

153. FIPS PUB 46-3, Data Encryption Standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, November 1999.
154. FIPS PUB 71, Key Management Using X9.17, National Institute of Standards and Technology, U.S. Department of Commerce, April 1992.

* DoD standards are available from: www.dodssp.daps.mil.

** FIPS PUBs are available from http://www.csrc.nist.gov.

155. FIPS PUB 74 (Parts 1–3), Guidelines for Implementing and Using the NBS Data Encryption Standard, National Bureau of Standards, U.S. Department of Commerce, April 1981.
156. FIPS PUB 81, DES Modes of Operation, National Bureau of Standards, U.S. Department of Commerce, December 1980.
157. FIPS PUB 102, Guidelines for Computer Security Certification and Accreditation, National Bureau of Standards, U.S. Department of Commerce, September 1983. (*Note:* This is currently being rewritten by NIST.)
158. FIPS PUB 112, Password Usage, National Bureau of Standards, U.S. Department of Commerce, May 1985.
159. FIPS PUB 113, Computer Data Authentication, National Bureau of Standards, U.S. Department of Commerce, May 1985.
160. FIPS 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, U.S. Department of Commerce, (draft) November 1999.
161. FIPS PUB 171, Key Management Using ANSI X9.17, National Institute of Standards and Technology, U.S. Department of Commerce, April 1992.
162. FIPS PUB 180-1, Secure Hash Standard, National Institute of Standards and Technology, U.S. Department of Commerce, April 1995.
163. FIPS PUB 181, Automated Password Generator, National Institute of Standards and Technology, U.S. Department of Commerce, October 1993.
164. FIPS PUB 185, Escrowed Encryption Standard, National Institute of Standards and Technology, U.S. Department of Commerce, February 1994.
165. FIPS PUB 186-2, Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, February 2000.
166. FIPS PUB 188, Standard Security Labels for Information Transfer, National Institute of Standards and Technology, U.S. Department of Commerce, September 1994.
167. FIPS PUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives, National Institute of Standards and Technology, U.S. Department of Commerce, September 1994.
168. FIPS 191, Guideline for the Analysis of Local Area Network Security, National Institute of Standards and Technology, U.S. Department of Commerce, November 1994.
169. FIPS PUB 196, Entity Authentication Using Public Key Cryptography, National Institute of Standards and Technology, U.S. Department of Commerce, February 1997.
170. Clipper Chip Technology, National Institute of Standards and Technology, U.S. Department of Commerce, April 1993.
171. Capstone Chip Technology, National Institute of Standards and Technology, U.S. Department of Commerce, April 1993.
172. Federal Criteria for Information Technology (IT) Security, version 1.0, National Institute of Standards and Technology, U.S. Department of Commerce, 1992.
173. Report on the Development of the Advanced Encryption System (AES), National Institute of Standards and Technology, U.S. Department of Commerce, October 2000.
174. SP 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, National Institute of Standards and Technology, U.S. Department of Commerce, October 2000.
175. SP 800-24, PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, National Institute of Standards and Technology, U.S. Department of Commerce, October 2000.

*U.S. Laws and Regulations**

176. Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, No. 040-000-00699-1, October 1997.

177. Cyberspace Electronic Security Act (CESA) of 1999.
178. National Information Infrastructure Protection Act of 1996, Title 18 USC Section 1030.

Commercial Standards

179. PKCS #1 v2.1: RSA Cryptography Standard.
180. PKCS #3: Diffie-Hellman Key-Agreement Standard.
181. PKCS #5 v2.0: Password-Based Cryptography Standard.
182. PKCS #6: Extended-Certificate Syntax Standard.
183. PKCS #7: Cryptographic Message Syntax Standard.
184. PKCS #8: Private-Key Information Syntax Standard.
185. PKCS #9 v2.0: Selected Object Classes and Attribute Types.
186. PKCS #10 v1.7: Certification Request Syntax Standard.
187. PKCS #11 v2.11: Cryptographic Token Interface Standard.
188. PKCS #12 V1.0: Personal Information Exchange Syntax.
189. PKCS #13: Elliptic Curve Cryptography Standard.
190. PKCS #15: Conformance Profile Specification.
191. PKCS #15 v1.1 Cryptographic Token Information Syntax Standard.
192. STR-SECURITY-01.00, ATM Security Specification, The ATM Forum Technical Committee, version 1.0, December 1997.

C.2 Publications

193. Ackerman, R., Security agency transitions from backer to participant, *SIGNAL*, October 1999, 23–25.
194. Ackerman, R., Hidden hazards menace U.S. information infrastructure, *SIGNAL*, August 1999, 17–20.
195. Ackerman, R., German firm aims antennas at security communications, *SIGNAL*, August 1999, 75–77.
196. Ackerman, R., Justice Department readies infrastructure defense plans, *Information Assurance Series*, AFCEA International Press, 1998, 4–31.
197. Ackerman, R., Europe seeks overarching view of information war, *Information Assurance Series*, AFCEA International Press, 1998, 15–16.
198. Ackerman, R., Government-industry gridlock hampers information security, *Information Assurance Series*, AFCEA International Press, 1998, 25–27.
199. Adams, C. and Lloyd, S., *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*, Macmillan Technical Publishing, 1999.
200. Amin, M., Toward self-healing infrastructure systems, *Computer*, 33(8), 44–53, 2000.
201. Amoroso, E., *Fundamentals of Computer Security Technology*, Prentice-Hall, 1994.
202. Arbaugh, W., Davin, J., Farber, D., and Smith, J., Security for virtual private intranets, *Computer*, 31(9), 48–56, 1998.
203. Arnold, R. and Bohner, S., *Software Change Impact Analysis*, IEEE, 1996.
204. Asokan, N., Janson, P., Steiner, M., and Waidner, M., The state of the art in electronic payment systems, *Computer*, 30(9), 28–35, 1997.
205. Atkins, D., Buis, P., Harc, C., Kelley, R., Nachenberg, C., Nelson, A., Phillips, P., Richey, T., Sheldon, T., and Snyder, J., *Internet Security Professional Reference*, 2nd ed., New Riders, 1997.

---

* U.S. Regulations are available from: The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, D.C. 20402-9328, U.S.A.

206. Ayton, P. and Hardman, D, Understanding and communicating risk: a psychological overview, *Safety-Critical Systems: The Convergence of High Tech and Human Factors*, Springer-Verlag, 1996, 168–183.
207. Babington, C., Clinton plan targets cyber-terrorism, *The Washington Post*, January 8, 2000, E1.
208. Barber, B., The European approach to standards in medical informatics, *Safety-Critical Systems*, Chapman & Hall, 1993, 238–254.
209. Barrell, T. and Darlison, T., The safety of PES in the offshore industry, *Safety and Reliability of Software Based Systems*, Springer-Verlag, 1995, 201–216.
210. Bass, T., Cyberspace situational awareness demands mimic traditional command requirements, *SIGNAL*, 54(6), 83–84, 2000.
211. Bernstein, T., Bhimani, A., Schultz, E., and Siegel, C., *Internet Security for Business*, John Wiley & Sons, 1996.
212. Besnard, J., Keene, S., and Voas, J., Assuring COTS products for reliability and safety critical systems, *Proceedings of the Annual Reliability & Maintainability Symposium*, IEEE, 1999, 317–322.
213. Birman, K., The next-generation Internet: unsafe at any speed?, *Computer*, 33(8), 54–60, 2000.
214. Black, H., Nolan, J., and Nolan-Haley, J., *Black's Law Dictionary*, 6th ed., West Publishing Company, 1990.
215. Blackburn, N., Can you keep a secret?, *The Jerusalem Post*, September 10, 1999, 28–29.
216. Blakley, B., *CORBA Security: An Introduction to Safe Computing with Objects*, Addison-Wesley, 2000.
217. Blancharski, D., *Network Security in a Mixed Environment*, IDG Books, 1999.
218. Bond, J., Silence is not golden, *Safety Systems*, September 1999, 12–15.
219. Boslaugh, D., *When Computers Went to Sea: The Digitalization of the U.S. Navy*, IEEE Computer Society Press, 1999.
220. Bott, T., Evaluating the risk of industrial espionage, *Proceedings of the Annual Reliability & Maintainability Symposium*, IEEE, 1999, 230–237.
221. Bouissou, M., Martin, F., and Ourghanlian, A., Assessment of a safety-critical system including software: a Bayes-belief network for evidence sources, *Proceedings of the Annual Reliability & Maintainability Symposium*, IEEE, 1999, 142–150.
222. Bowen, J. and Hinchey, M., *High-Integrity System Specification and Design*, IEEE Computer Society Press, 1999.
223. Bradley, K., Cheung, S., Puketza, N., Mukherjee, B., and Olsson, R., Detecting disruptive routers: a distributed network monitoring approach, *IEEE Symposium on Security and Privacy*, 1998, 115–124.
224. Branscomb, L. and Keller, J. (Eds.), *Converging Infrastructures: Intelligent Transportation Systems and the National Information Infrastructure*, MIT Press, 1996.
225. Brewer, D., Applying security techniques to achieving safety, *Directions in Safety-Critical Systems*, Springer-Verlag, 1993, 246–256.
226. Briscoe, G., U.S. DoE Computerized Accident/Incident Reporting System (CAIRS), *Proceedings, 11th International System Safety Society Conference*, 1993, 2.C-2-1–2.C-2-8.
227. Brown, D., Government efforts confound commercial wireless security, *Information Assurance Series*, AFCEA International Press, 1998, 29–31.
228. Brown, D., Gunderson, L., and Evans, M., Interactive analysis of computer crimes, *Computer*, 33(6), 69–77, 2000.
229. Brune, K., Security Improvement Modules: Securing Networks Using Best Practices, *news@sei*, Carnegie Melon University Software Engineering Institute, 1(2), 2–3, 1998.
230. Burnett, R., Anticipate and prevent — managing legal risks in safety-critical systems, *Safety-Critical Systems: The Convergence of High Tech and Human Factors*, Springer-Verlag, 1996, 139–152.

231. Campen, A., National vulnerability intensifies as infrastructure reliance grows, *Information Assurance Series*, AFCEA International Press, 1998, 6–7.
232. Campen, A., It's vulnerability, not threat — stupid!, *Information Assurance Series*, AFCEA International Press, 1998, 28–31.
233. Campen, A., Information systems and air warfare, Campen, A. (Ed.), *The First Information War*, AFCEA International Press, 1992, 23–25.
234. Campen, A., Communications support to intelligence, Campen, A. (Ed.), *The First Information War*, AFCEA International Press, 1992, 51–60.
235. Campen, A., Information, truth, and war, Campen, A. (Ed.), *The First Information War*, AFCEA International Press, 1992, 87–91.
236. Campen, A., Technology did not create and cannot resolve privacy dilemma, *SIGNAL*, 54(5), 39–40, 2000.
237. Capell, P., Analysis of Courses in Information Management and Network System Security and Survivability, CMU/SEI-99-SR-006.
238. Caplan, K. and Sanders, J., Building an international security standard, *IT Professional*, 1(2), 29–34, 1999.
239. Chadwick, D., Smart cards aren't always the smart choice, *Computer*, 32(12), 142–143, 1999.
240. Chapman, D. and Zwicky, E., *Building Internet Firewalls*, 1st ed., O'Reilly & Associates, 1995.
241. Cheswick. W. and Bellovin, S., *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994.
242. Chillon, B., *Design Reliability: Fundamentals and Applications*, CRC Press, 1999.
243. Clark, D., Encryption advances to meet internet challenges, *Computer*, 33(8), 20–24, 2000.
244. Cohen, F., *Protection & Security on the Information Superhighway*, John Wiley & Sons, 1995.
245. Cohen, F., *A Short Course on Computer Viruses*, 2nd ed., John Wiley & Sons, 1994.
246. Cook, R., Management of dependability: a railway perspective, *Safety-Critical Systems: The Convergence of High Tech and Human Factors*, Springer-Verlag, 1996, 61–70.
247. Davies, B., Safety of medical robots, *Safety-Critical Systems*, Chapman & Hall, 1993, 193–201.
248. Denning, D., *Information Warfare and Security*, Addison-Wesley, 1999.
249. Denning, D., *Cryptography and Data Security*, Addison-Wesley, 1982.
250. Deswarte, Y., Dependable computing system evaluation criteria: SQUALE proposal, Weinstock, C. and Rushby, J. (Eds.), *Dependable Computing for Critical Applications 7*, IEEE, 1999, 397–400.
251. Dima, A., Wack, J., and Wakid, S., Raising the bar on software security testing, *IT Professional*, 1(3), 27–32, 1999.
252. Doraswamy, N. and Harkins, D., *IPSec: The New Security Standard for the Internet, Intranet, and Virtual Private Networks*, Prentice-Hall, 1999.
253. Dowd, P. and McHenry, J., Network security: it takes time to take it seriously, *Computer*, 31(9), 24–28, 1998.
254. Dreifus, H. and Monk, J., *Smartcards: A Guide to Building and Managing Smartcard Applications*, John Wiley & Sons, 1997.
255. Duetertre, B. and Stavridou, V., A Model of noninterference for integrating mixed-criticality software components, Weinstock, C. and Rushby, J. (Eds.), *Dependable Computing for Critical Applications 7*, IEEE, 1999, 301–316.
256. Elliott, J., System engineering and safety-related systems, *Safety Systems*, 7(3), 14–16, 1998.
257. Ellison, F., Fisher, D., Linger, R., Lipson, H., Longstaff, T., and Mead, N., Survivable Network Systems: An Emerging Discipline, CMU/SEI-97-TR-013.

258. Escamilla, T., *Intrusion Detection: Security Beyond the Firewall*, John Wiley & Sons, 1998.
259. Falla, M. (Ed.), Advances in Safety Critical Systems: Results and Achievements from the DTI/EPSRC R&D Programme in Safety Critical Systems, June 1997.
260. Feghi, J., Feghi, J., and Williams, P., *Digital Certificates: Applied Internet Security*, Addison-Wesley, 1998.
261. Firth, R., Fraser, B., Konda, S., and Simmel, D., An Approach for Selecting and Specifying Tools for Information Survivability, CMU/SEI-97-TR-009.
262. Ford, W. and Baum, M., *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice-Hall, 1997.
263. Fox, J., Das, S., Elsdon, D., and Hammond, P., Decision making and planning by autonomous agents: a generic architecture for safety-critical applications, *Safety and Reliability of Software Based Systems*, Springer-Verlag, 1995, 122–134.
264. Fraser, T., Badger, L., and Feldman, M., Hardening COTS software with generic software wrappers, *IEEE Symposium on Security and Privacy*, 1999.
265. Friedman, M. and Voas, J., *Software Assessment: Reliability, Safety, Testability*, John Wiley & Sons, 1995.
266. Frischholz, R. and Dieckmann, U., BioID: a multimodal biometric identification system, *Computer*, 33(2), 64–69, 2000.
267. Frith, K. and Ellis, R., Artificial intelligence — genuine hazards, *Safer Systems*, Springer-Verlag, 1997, 79–95.
268. Garber, L., News Briefs: U.S. seeks encryption standard, *Computer*, 31(7), 20, 1998.
269. Garber, L., News Briefs: Satellite processor failure cuts Net, pager service, *Computer*, 31(7), 19–20, 1998.
270. Garber, L., News Briefs: Private doorbells for encryption, *Computer*, 31(10), 17–18, 1998.
271. Garber, L., News Briefs: Companies join forces for smart-card standard, *Computer*, 31(11), 19–20, 1998.
272. Garber, L., Melissa virus creates a new type of threat, *Computer*, 32(6), 16–19, 1999.
273. Garfinkel, S., *Web Security and Commerce*, 1st ed., O'Reilly & Associates, 1997.
274. Garfinkel, S. and Spafford, G., *Practical UNIX and Internet Security*, 2nd ed., O'Reilly & Associates, 1998.
275. Garfinkel, S., *PGP: Pretty Good Privacy*, 1st ed., O'Reilly & Associates, 1994.
276. Ghosh, A., *E-Commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, 1998.
277. Gollmann, D., *Computer Security*, John Wiley & Sons, 1999.
278. Gong, L., *Inside Java™ 2 Platform Security: Architecture, API Design, and Implementation*, Addison-Wesley, 1999.
279. Goodden, R., Business strategies for the information age, Campen, A., Dearth, D., and Goodden, R. (Eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age*, AFCEA International Press, 1996, 133–145.
280. Gordon, B., What's in a name? A password, *The Jerusalem Post*, August 25, 2000, 28–29.
281. Groner, E., Checkpoint forms unit for home net security, *The Jerusalem Post*, December 24, 1999, p. 29.
282. Hankins, M., Trusted gate closes on thin-client computer network security holes, *SIGNAL*, December 1999, 67–69.
283. Hankins, M., Integrated circuit chip provides secure, rapid data encryption, *SIGNAL*, October 1999, 47–48.
284. Hankins, M., Standards Institute studies encoding formula options, *SIGNAL*, August 1999, 69–72.
285. Hankins, M., Layered approach security planning offers best defense against attacks, *SIGNAL*, 54(8), 55–57, 2000.

286. Harrison, R., *ASP/MTS/ADSI: Web Security*, Prentice-Hall, 1999.
287. Herrinshaw, C., Detecting attacks on networks, *Computer*, 30(12), 16–17, 1997.
288. Herrmann, D., *Software Safety and Reliability: Techniques, Approaches and Standards of Key Industrial Sectors*, IEEE Computer Society Press, 1999.
289. Herrmann, D. and Peercy, D., Software reliability cases: the bridge between hardware, software, and system safety and reliability, *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS'99)*, IEEE, 1999.
290. Herrmann, D., Software safety and reliability concerns in the ground-based transportation industry, *Proceedings of the 16th International System Safety Society Conference*, September 14–19, 1998, Seattle, WA, 248–255.
291. Herrmann, D., Software safety: the medical perspective, invited tutorial for the *16th International System Safety Society Conference*, September 14–19, 1998, Seattle, WA.
292. Herrmann, D., Sample implementation of the Littlewood holistic model for analyzing software safety and reliability, *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS'98)*, IEEE, 1998.
293. Herrmann, D. and Zier, D., Using IEC 601-1-4 to satisfy the requirements of the FDA software guidance, *Medical Device & Diagnostic Industry*, December 1995, 104–107.
294. Herrmann, D., Standards for high integrity systems, invited presentation to *IEEE International Software Engineering Standards Symposium (ISESS '95)*, Montreal, Quebec, August 21–25, 1995.
295. Herrmann, D., A methodology for evaluating, comparing, and selecting software safety and reliability standards, *Proceedings of the 10th Annual Conference on Computer Assurance, Systems Integrity, and Software Safety (COMPASS '95)*, IEEE, June 1995, Washington, D.C., 223–232.
296. Herrmann, D., A preview of IEC safety requirements for programmable electronic medical systems, *Medical Device & Diagnostic Industry*, June 1995, 106–110.
297. Herrmann, D., Using EN 60601-1-4 to satisfy the requirements of the FDA software guidance, *Proceedings of the EuroSpec Institute for Equipment Safety, Software Validation Seminar*, Heidelberg, Germany, June 1–2, 1995.
298. Herrmann, D., Software Safety and Reliability in the Regulatory Environment, Health Industries Manufacturers Association (HIMA) Report No. 95-8, 1995, tab 8, 1–59.
299. Herrmann, D., IEC (DIS) 601-1-4 Safety Requirements for Programmable Electronic Medical Systems, *Proceedings of 5th Annual Association for Advancement of Medical Instrumentation (AAMI) International Standards Conference*, Washington, D.C., March 16–17, 1995, 425–458.
300. Hessami, A., Risk: a holistic business perspective, *Industrial Perspectives of Safety-Critical Systems*, Springer-Verlag, 1998, 112–125.
301. Holden, T., Glykas, M., Wilhelmij, P., and Reynolds, B., Lifetrack: organizational modelling for safety-critical decision support, *Technology and Assessment of Safety-Critical Systems*, Springer-Verlag, 1994, 79–102.
302. Hutt, A., Bosworth, S., and Hoyt, D., *Computer Security Handbook*, 3rd ed., John Wiley and Sons, 1995.
303. Icove, D., Seger, K., and VonStorch, W., *Computer Crime: A Crime Fighter's Handbook*, O'Reilly & Associates, 1995.
304. Jackson, D., Social issues in high-tech safety, *Technology and Assessment of Safety-Critical Systems*, Springer-Verlag, 1994, 164–174.
305. Jajodia, S., Ammann, P., and McCollum, C., Surviving information warfare attacks, *Computer*, 32(4), 57–63, 1999.
306. *Janes Military Communications*, 18th ed., 1997–1998, Jane's Defense Reference.
307. Jensen, F., *An Introduction to Bayesian Belief Networks*, Springer-Verlag, 1996.
308. Jesty, P., Safety issues for future intelligent transport systems, *Safety Systems*, 8(1), 1–3, 1998.

309. Jesty, P. and Buckley, T., Toward safe road-transport informatic systems, *Safety-Critical Systems*, Chapman & Hall, 1993, 297–311.
310. Johnson, D., Increasing software integrity using functionally dissimilar monitoring, *Safer Systems*, Springer-Verlag, 1997, 216–230.
311. Jones, A., The challenge of building survivable information-intensive systems, *Computer*, 33(8), 39–43, 2000.
312. Kahin, B. and Nesson, C., *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, MIT Press, 1997.
313. Kaufman, C., Perlman, R., and Speciner, M., *Network Security: Private Communication in a Public World*, Prentice-Hall, 1995.
314. Kaufman, E. and Newman, A., *Implementing IPSec*, John Wiley & Sons, 1999.
315. Kenyon, H., Prototype code connects multitude of security devices, *SIGNAL*, November 1999, 63–64.
316. Kippenhahn, R., *Code Breaking: A History and Exploration*, Overlook, 1999.
317. Knight, J., Elder, M., and Du, X., Error recovery in critical infrastructure systems, *Computer Security, Dependability, and Assurance: From Needs to Solutions*, IEEE, 1999, 49–71.
318. Knott, S., *Secret and Sanctioned: Covert Operations and the American Presidency*, Oxford University Press, 1996.
319. Kochmar, J., Allen, J. Alberts, C., Cohen, C., Ford, G., Fraser, B., Konda, S., Kossakowski, K., and Simmuel, D., Preparing to Detect Signs of Intrusion, Security Improvement Module, CMU/SEI-SIM-005, 1998.
320. Koorneef, F., Spijkervet, A., and Karczewski, J., Organizational learning using near-miss and accident data within and outside your organization, *Safety-Critical Systems: The Convergence of High Tech and Human Factors*, Springer-Verlag, 1996, 153–167.
321. Ladkin, P., Why–because analysis, *Safety Systems*, January 2000, 1–4.
322. Lang, B. and Pesante, L., CERT Coordination Center celebrates ten years, *news@sei*, Carnegie Melon University Software Engineering Institute, 1(3), 6–7, 1998.
323. Laswell, B., Simmel, D., and Behrens, S., Information Assurance Curriculum: State of the Practice, CMU/SEI-99-TR-21.
324. Latino, R. and Latino, K., *Root Cause Analysis: Improving Performance for Bottom Line Results*, CRC Press, 1999.
325. Lawson, H., An assessment methodology for safety critical computer based systems, *Safety and Reliability of Software Based Systems*, Springer-Verlag, 1995, 183–200.
326. Lawson, H., Infrastructure risk reduction, *Communications of the ACM*, 40(6), 120, 1998.
327. Lawton, G., Intellectual property protection opens path for E-commerce, *Computer*, 33(2), 14–21, 2000.
328. Lear, A., News Briefs: Explorer worm targets networks, *Computer*, 32(8), 15, 1999.
329. Lear, A., News Briefs: Encryption industry grows outside U.S., *Computer*, 32(8), 16, 1999.
330. Lee, T., Cryptography and the new economy, *Industrial Physicist*, 6(4), 29–33, 2000.
331. Lehtinen, M. and Lear, A., Intrusion detection: managing the risk of connectivity, *IT Professional*, 1(6), 11–13, 1999.
332. Lerner, E., Biometric identification, *The Industrial Physicist*, 6(1), 20–23, 2000.
333. Leveson, N., *Safeware: System Safety and Computers*, Addison-Wesley, 1995.
334. Levi, S.T. and Agrawala, A., *Fault Tolerant System Design*, McGraw-Hill, 1994.
335. Lindquist, U. and Jonsson, E., A map of security risks associated with using COTS, *Computer*, 31(6), 60–66, 1998.
336. Linger, R., Survivable network analysis: assessing the survivability of critical systems, *news@sei*, Carnegie Melon University Software Engineering Institute, 2(2), 10–11, 1999.
337. Littlewood, B., The need for evidence from disparate sources to evaluate software safety, *Directions in Safety-Critical Systems*, Springer-Verlag, 1993, 217–231.
338. Lloyd, I. and Simpson, M., Computer risks and some legal consequences, *Safety and Reliability of Software Based Systems*, Springer-Verlag, 1995, 378–388.

339. Long, F., Hissam, S., Seacord, R., and Robert, J., Securing Internet Sessions with Sorbet, CMU/SEI-99-TN-002.
340. Long, R. and Briant, V., Vigilance required: lessons for creating a strong nuclear culture, *Journal of System Safety*, 35(4), 31–34, 1999.
341. Loomes, M., Ridley, D., and Kornbrot, D., Cognitive and organizational aspects of design, *Technology and Assessment of Safety-Critical Systems*, Springer-Verlag, 1994, 186–193.
342. Lynch, D. and Lundquist, L., *Digital Money: the New Era of Internet Commerce*, John Wiley & Sons, 1995.
343. Lyu, M. (Ed.), *Handbook of Software Reliability Engineering*, IEEE Computer Society Press, 1996.
344. Martin, J., *Design and Strategy for Distributed Data Processing*, Prentice-Hall, 1981.
345. McDermid, J., Issues in the development of safety-critical systems, *Safety Critical Systems*, Chapman & Hall, 1993, 16–42.
346. McDysan, D., *VPN Applications Guide: Real Solutions for Enterprise Networks*, John Wiley & Sons, 2000.
347. McGraw, G. and Felten, E., *Securing Java: Getting Down to Business with Mobile Code*, 2nd ed., John Wiley & Sons, 1999.
348. McGraw, G., Software Assurance for Security, *Computer*, 32(4), 103–105, 1999.
349. McGraw III, H., Online privacy: self-regulate or be regulated, *IT Professional*, 1(2), 18–19, 1999.
350. McSteen, B. and Pesante, L., The CERT knowledge base: organizing vulnerability information, *news@sei*, Carnegie Melon University Software Engineering Institute, 1(1), 12–14, 1998.
351. Measuring and predicting software safety and reliability, *IMPACT*, Engineering and Physical Sciences Research Council (EPSRC), No. 22, March 1999, p. 5.
352. Meeks, B., Privacy lost, anytime, anywhere, *Communications of the ACM*, 40(8), 11–13, 1997.
353. Menezes, A., Van Oorschot, P., and Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, 1996.
354. Merkow, M., Breithaupt, J., and Wheeler, K., *Building SET Applications for Secure Transactions*, John Wiley & Sons, 1998.
355. Microsoft, Security in the Internet age, *The Washington Post*, 24 January 2000, p. A8.
356. Mills, S., Integrated marine navigation systems — problems of operation, *Safety Systems*, 8(1), 4–6, 1998.
357. Morris, D., *Introduction to Communication Command and Control Systems*, Pergamon Press, 1977.
358. Musa, J., *Software Reliability Engineering*, McGraw-Hill, 1999.
359. Negin, M., Chmieliewski, T., Salganicoff, M., Camus, T., von Seelen, U., Venetianer, P., and Zhang, G., An iris biometric system for public and personal use, *Computer*, 33(2), 70–75, 2000.
360. Neil, M. and Fenton, N., Applying Bayesian Belief Networks to critical systems assessment, *Safety Systems*, 8(3), 10–13, 1999.
361. Neil, M., Littlewood, B., and Fenton, N., Applying Bayesian Belief Networks to system dependability assessment, *Safety-Critical Systems: The Convergence of High Tech and Human Factors*, Springer-Verlag, 1996, 71–94.
362. Neumann, P., *Computer Related Risks*, Addison-Wesley, 1995.
363. Neumann, P., Identity-related misuse, *Communications of the ACM*, 40(7), 112, 1997.
364. Neumann, P., Crypto key management, *Communications of the ACM*, 40(8), 136, 1997.
365. Neumann, P., Protecting the infrastructures, *Communications of the ACM*, 41(1), 128, 1998.
366. Nichols, D., *ICSA Guide to Cryptography*, McGraw-Hill, 1999.
367. Nordland, O., A discussion of risk tolerance principles, *Safety Systems*, 8(3), 1–4, 1999.

368. O'Connor, P., *Practical Reliability Engineering*, 3rd ed., John Wiley & Sons, 1991.
369. O'Sullivan, A., Bracing for cyber-war, *The Jerusalem Post*, June 4, 1999, 20–21.
370. Oppliger, R., *Authentication Systems for Secure Networks*, Artech House, 1996.
371. Oppliger, R., *Internet and Intranet Security*, Artech House, 1998.
372. Oppliger, R., Security at the Internet layer, *Computer*, 31(9), 43–47, 1998.
373. Ouellette, J., Detection on the cutting edge, *The Industrial Physicist*, 6(2), 8–12, 2000.
374. Pankanti, S., Bolle, R., and Jain, A., Biometrics: the future of identification, *Computer*, 33(2), 46–49, 2000.
375. Parker, D., *Fighting Computer Crime: A New Framework for Protecting Information*, John Wiley & Sons, 1998.
376. Parkin, G. and Wichmann, B., Reliability of smart instrumentation, *Safety Systems*, 8(2), 6–7, 1999.
377. Pegobaro, R., Digital devices steal the show, *The Washington Post*, January 8, 2000, pp. E1–E8.
378. Pentland, A. and Choudhury, T., Face recognition for smart environments, *Computer*, 33(2), 50–55, 2000.
379. Pesante, L. and Lang, B., FedCIRC: incident response for federal agencies, *news@sei*, Carnegie Melon University Software Engineering Institute, 2(1), 10–11, 1999.
380. Petroski, H., *To Engineer is Human: The Role of Failure in Successful Design*, Barnes & Noble, 1994.
381. Philley, J., A case for multiple root cause approach for incident investigation, *Proceedings, 11th International System Safety Society Conference*, 1993, 2.C-3-1–2.C-3-10.
382. Pfaffenberger, B., *Protect Your Privacy on the Internet*, John Wiley & Sons, 1997.
383. Pfleeger, C., *Security in Computing*, 2nd ed., Prentice-Hall, 1997.
384. Phillips, P., Martin, A., Wilson, C., and Przybocki, M., An introduction to evaluating biometric systems, *Computer*, 33(2), 56–63, 2000.
385. Poe, R., Accident investigation: the sooner the better, *Proceedings, 10th International System Safety Society Conference*, 1991, 4.4-6-1–4.4-6-8.
386. Power, R., *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare*, 3rd ed., Computer Security Institute, 1998.
387. Predicting software defects in consumer digital products, *Agena News*, Agena, Ltd., December 1999, 1.
388. Pritchard, M., Safeguarding systems: in-service management, *Industrial Perspectives of Safety-Critical Systems*, Springer-Verlag, 1998, 137–149.
389. Raheja, D., *Assurance Technologies: Principles and Practices*, McGraw-Hill, 1991.
390. Randell, B., Dependability — a unifying concept, *Computer Security, Dependability, and Assurance: From Needs to Solutions*, IEEE, 1999, 16–25.
391. Rathmell, A., Assessing the IW threat from sub-state groups, *Cyberwar 2.0: Myths, Mysteries and Reality*, Campen, A. and Dearth, D. (Eds.), AFCEA International Press, 1998, 295–312.
392. Redmill, F., Chudleigh, M., and Catmur, J., *System Safety: HAZOP and Software HAZOP*, John Wiley & Sons, 1999.
393. Rendell, A., Security, privacy, and fraud research, *Safety Systems*, 9(2), 13–15, 2000.
394. Review of Formal Methods for Specification, Verification, and Risk Analysis in Critical Systems, Agena Ltd., 1999 (*www.agena.co.uk*).
395. Rindfleisch, T., Privacy, information technology, and health care, *Communications of the ACM*, 40(8), 92–100, 1997.
396. Ritter, T., Cryptography: is staying with the herd really best?, *Computer*, 32(8), 94–95, 1999.
397. Robinson, C., Information superiority drives Pentagon policy and guidance, *Information Assurance Series*, AFCEA International Press, 1998, 8–11.
398. Robinson, C., U.S. seeks alliance support for infrastructure protection, *Information Assurance Series*, AFCEA International Press, 1998, 12–14.

399. Robinson, C., External network threats to decline as insiders pose more difficult issues, *Information Assurance Series*, AFCEA International Press, 1998, 14.
400. Robinson, C., Security product trust demands laboratory test and evaluation, *SIGNAL*, 54(8), 51–54, 2000.
401. Rona, T., From scorched earth to information warfare, Campen, A., Dearth, D., and Goodden, R. (Eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age*, AFCEA International Press, 1996, 9–11.
402. Rosenberg, D., The video phone comes of age, *The Jerusalem Post*, December 31, 1999, p. 28.
403. Rozenblit, M., *Security for Telecommunications Network Management*, IEEE, 1999.
404. Rubin, A., Geer Jr., D., and Ranum, M., *Web Security Sourcebook*, John Wiley & Sons, 1997.
405. Rubin, A. and Geer Jr., D., A survey of Web security, *Computer*, 31(9), 34–42, 1998.
406. Sander, T. and Tschudin, C., Towards mobile cryptography, *IEEE Symposium on Security and Privacy*, 1998, 215–224.
407. Schneier, B., *E-mail Security: How to Keep Your Electronic Messages Private*, John Wiley & Sons, 1995.
408. Schneier, B. and Banisar, D., *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, 1997.
409. Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, 1995.
410. Schneier, B., Cryptographic design vulnerabilities, *Computer*, 31(9), 29–33, 1998.
411. Schneier, B., Cryptography: the importance of not being different, *Computer*, 32(3), 108–112, 1999.
412. Scott, C., Wolfe, P., and Erwin, M., *Virtual Private Networks*, 2nd ed., O'Reilly & Associates, 1999.
413. Shuman, E., Just sign on the dotted screen, *The Jerusalem Post*, August 4, 2000, p. 29.
414. Sieber, U., *The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy*, John Wiley & Sons, 1986.
415. Skoglund, E., OSE — a safer RTOS, *Safety Systems*, 9(1), 7–9, 1999.
416. Slade, R., *Guide to Computer Viruses*, Springer-Verlag, 1994.
417. Smith, J., Using a layered functional model to determine safety requirements, *Safer Systems*, Springer-Verlag, 1997, 56–66.
418. Snow, A., Varshney, U., and Malloy, A., Reliability and survivability of wireless and mobile networks, *Computer*, 33(7), 49–55, 2000.
419. Stallings, W., *Cryptography and Network Security*, 2nd ed., Prentice-Hall, 1998.
420. Stamatis, D., *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, ASQC Press, 1995.
421. Stein, L., *Web Security*, Addison Wesley, 1998.
422. Storey, N., *Safety-Critical Computer Systems*, Addison-Wesley, 1996.
423. Strebe, M. and Edwards, M., *NT Network Security*, Sybex, Inc., 1999.
424. Summers. R., *Secure Computing: Threats and Safeguards*, McGraw-Hill, 1997.
425. System Safety Society, *System Safety Analysis Handbook*, 2nd ed., July 1997.
426. Tarman, T., Hutchinson, R., Pierson, L., Sholander, P., and Witzke, E., Algorithm-agile encryption in ATM networks, *Computer*, 31(9), 57–64, 1998.
427. Tilton, C., An emerging biometric API industry standard, *Computer*, 33(2), 130–132, 2000.
428. Tiwana, A., *Web Security*, Digital Press, 1999.
429. Toigo, J., *Disaster Recovery Planning for Computers and Communications Resources*, John Wiley & Sons, 1996.
430. Toma, J., Desert Storm communications, Campen, A. (ed.), *The First Information War*, AFCEA International Press, 1992, 1–5.

431. TRACS: Assessing military vehicle reliability, *Agena News*, Agena, Ltd., December 1999, 2–3.
432. Tran, T., Murdock, W., and Pohl, E., Bayes analysis for system-reliability inferences, *Proceedings of the Annual Reliability & Maintainability Symposium*, IEEE, 1999, 151–157.
433. Tung, B., *Kerberos: A Network Authentication System*, Addison-Wesley, 1999.
434. Underwood, A., A framework for certifying critical software systems, *Safety and Reliability of Software Based Systems*, Springer-Verlag, 1995, 419–438.
435. Voas, J. and McGraw, G., *Software Fault Injection*, John Wiley & Sons, 1998.
436. Wang, H., Lee, M., and Wang, C., Consumer Privacy Concerns about Internet Marketing, *Communications of the ACM*, 41(3), 63–70, 1998.
437. Wayman, J., Federal biometric technology legislation, *Computer*, 33(2), 76–81, 2000.
438. West-Brown, M., Stikvoort, D., and Kossakowski, K., *Handbook for Computer Security Incident Response Teams*, CMU/SEI-98-HB-001.
439. Whetton, C., Maintainability and its influence on system safety, *Technology and Assessment of Safety-Critical Systems*, Springer-Verlag, 1994, 31–54.
440. Whittey, R., Product monitoring for integrity and safety enhancement, *Safer Systems*, Springer-Verlag, 1997, 256–274.
441. Wiener, L., *Digital Woes*, Addison-Wesley, 1993.
442. Wood, N., Real partnership critical to infrastructure protection, *Information Assurance Series*, AFCEA International Press, 1998, 3.
443. Wood, N., The world needs an international approach to information security, *SIGNAL*, August 1999, 14.
444. Wylie, J. et al., Survivable Information Storage Systems, *Computer*, 33(8), 61–68, 2000.
445. Zebroski, E., Lessons learned from catastrophes, *Risk Management: Expanding Horizons in Nuclear Power and Other Industries*, Knief, R. et al. (Eds.), Hempshire Publishing, 1991.
446. Zhong, Q. and Edwards, N., Security control for COTS components, *Computer*, 31(6), 67–73, 1998.

C.3 Online Resources

The following online resources, which were accurate at the time of writing, provide current information about a variety of issues related to information assurance.

447. *http://csrc.nist.gov/cryptval*; information about NIST cryptographic validation program.
448. *http://csrc.nist.gov/welcome.html*; NIST computer security clearinghouse.
449. *http://java.sun.com/forum/securityforum.html*; Java™ security information.
450. *http://members.xoom.com/_xoom/InfoSysSec/index.html*; computer, network, telecommunications and physical security information from Algonquin College.
451. *http://niap.nist.gov*; information about NIAP program and firewall testing.
452. *http://service.symantec.com*; commercial virus protection products (Norton) and latest virus news.
453. *http://web.mit.edu/kerberos/www/index.html*; official Kerberos Web page.
454. *safety-critical@cs.york.ac.uk*; software safety discussion group, send e-mail to join.
455. *www.acm.org*; ACM Risks Forum.
456. *www.afiwc.aia.af.mil*; USAF Information Warfare Center.
457. *www.agena.co.uk*; BBN articles and tutorials, risk management research.
458. *www.asisonline.com*; American Society of Industrial Security.
459. *www.biometrics.org*; Biometric Consortium Web site.

460. *www.cert.org*; CMU SEI Computer Emergency Response Team Coordination Center studies Internet security vulnerabilities, provides incident response services, publishes security alerts, researches security and survivability in wide-area computing.
461. *www.certicom.com*; cryptography white papers.
462. *www.configate.com*; biometric authentication through voice verification.
463. *www.counterpane.com*; cryptography newsletter and related information.
464. *www.cerias.purdue.edu*; Center for Education and Research in Information Assurance and Security.
465. *www.csrc.nist.gov/encryption/aes*; information about advanced encryption standard (AES).
466. *www.cybersafe.com*; commercial distributor of Kerberos.
467. *www.epic.org*; Electronic Privacy Information Center.
468. *www.fbi.gov/nipc/index.htm*; U.S. National Infrastructure Protection Center.
469. *www.fedcirc.gov*; Computer Incident Response Center for U.S. federal government.
470. *www.gocsi.com*; Computer Security Institute Web site.
471. *www.iatf.net/*; Information Assurance Technical Framework Forum.
472. *www.htcn.org/*; High Tech Crime Network.
473. *www.hugin.com*; automated BBN tool.
474. *www.ibia.org*; International Biometric Industry Association Web site.
475. *www.ietf.org*; Internet Engineering Task Force Web site.
476. *www.iss.net*; Internet Security Systems.
477. *www.jedefense.com*; Journal of Electronic Defense.
478. *www.kerberos.isi.edu*; Kerberos information.
479. *www.mcafee.com*; commercial virus protection products and latest virus news.
480. *www.microsoft.com/security*; information about security features, security alerts, and patches to operating systems.
481. *www.netscape.com/eng/ssl3*; SSL information.
482. *www.nsi.org*; National Security Institute's security resources.
483. *www.omg.org*; CORBA information and specifications.
484. *www.pccip.gov*; (U.S.) President's Commission on Critical Infrastructure Protection.
485. *www.privacy.org*; Internet Privacy Coalition.
486. *www.protonworld.com*; joint venture that is developing an open smart card standard.
487. *www.psycom.net/iwar.1.html*; Institute for the Advanced Study of Information Warfare.
488. *www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html*; information about the Common Criteria for IT Security Evaluation (CCITSE).
489. *www.rsa.com*; RSA Data Security.
490. *www.rvs.uni-bielefeld.de*; why–because analysis home page, commercial aviation safety Web site.
491. *www.safety-club.org.uk*; Web site of Safety-Critical Systems Club and Software Reliability and Metrics Club, sponsored by the Centre for Software Reliability.
492. *www.sans.org*; System Administration, Networking and Security Institute.
493. *www.setco.org*; SET Secure Electronic Transaction specification, version 1.0, May 31, 1997.
494. *www.spa.org*; Software Publishers Association.
495. *www.symantec.com/avcenter*; Symantec antivirus research center.
496. *www.system-safety.org*; Web site of System Safety Society.
497. *www.terrorism.com/infowar/index.html*; the Terrorism Research Center.
498. *www.tis.com*; Trust Information Systems, Inc.
499. *www.verisign.com*; VeriSign Corporation.
500. *www.sse-cmm.org/librarie.htm*; latest information about SSE-CMM.
501. *www.issea.org*; latest information about SSE-CMM.