Appendix C

REFERENCES

GOVERNMENT REFERENCES

FAA Order 1810, Acquisition Policy

FAA Order 8040.4 FAA Safety Risk Management

FAA Advisory Circular 25.1309 (Draft), System Design and Analysis, January 28, 1998

RTCA-DO 178B, Software Considerations In Airborne Systems And Equipment Certification, December 1, 1992 COMDTINST M411502D, System Acquisition Manual, December 27, 1994DODD 5000.1, Defense Acquisition, March 15, 1996

DOD 5000.2R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems, March 15, 1996

DOD-STD 2167A, Military Standard Defense System Software Development, February 29, 1988

MIL-STD 882D, System Safety Program Requirements, February 10, 2000

MIL-STD 498, Software Development and Documentation, December 5, 1994

MIL-HDBK-217A, “Reliability Prediction of Electronic Equipment,” 1982.

MIL-STD-1629A “Procedures for Performing a Failure Mode, Effects and Criticality Analysis,” November 1980.

MIL-STD-1472D, “Human Engineering Design Criteria for Military Systems, Equipment and Facilities,” 14 March 1989.

NSS 1740.13, Interim Software Safety Standard, June 1994

29 CFR 1910.119 Process Safety Management, U.S. Government Printing Office, July 1992.

Department of the Air Force, Software Technology Support Center, Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems, Version-2, June 1996, Volumes 1 and 2 AFISC SSH 1-1, Software System Safety Handbook, September 5, 1985

Department of Defense, AF Inspections and Safety Center (now the AF Safety Agency), AFIC SSH 1-1 “Software System Safety,” September 1985.

Department of Labor, 29 CFR 1910, “OSHA Regulations for General Industry,” July 1992.

Department of Labor, 29 CFR 1910.119, “Process Safety Management of Highly Hazardous Chemicals,” Federal Register, 24 February 1992.

Department of Labor, 29 CFR 1926, “OSHA Regulations for Construction Industry,” July 1992.

Department of Labor, OSHA 3133, “Process Safety Management Guidelines for Compliance,” 1992.

Department of Labor, OSHA Instructions CPL 2-2.45A, Compliance Guidelines and Enforcement Procedures, September 1992.

Department of Transportation, DOT P 5800.5, “Emergency Response Guidebook,” 1990.

Environmental Protection Agency, 1989d, Exposure Factors Handbook, EPA/600/8-89/043, Office of Health and Environmental Assessment, Washington, DC 1989.

Environmental Protection Agency, 1990a, Guidance for Data Usability in Risk Assessment, EPA/540/G-90/008, Office of Emergency and Remedial Response, Washington, DC 1990.

COMMERICIAL REFERENCES

ACGIH, “Guide for Control of Laser Hazards,” American Conference of Government Industrial Hygienists, 1990.

American Society for Testing and Materials (ASTM), 1916 Race Street, Philadelphia, PA. 19103

ASTM STP762, “Fire Risk Assessment” American Society for Testing Materials, 1980.

EIA-6B, G-48, Electronic Industries Association, System Safety Engineering In Software Development1990 IEC 61508: International Electrotechnical Commission. Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems, December 1997

EIC 1508 -(Draft), International Electrotechnical Commission, Functional Safety; Safety-Related System, June 1995

IEEE STD 1228, Institute of Electrical and Electronics Engineers, Inc., Standard For Software Safety Plans, 1994

IEEE STD 829, Institute of Electrical and Electronics Engineers, Inc., Standard for Software Test Documentation, 1983

IEEE STD 830, Institute of Electrical and Electronics Engineers, Inc., Guide to Software Requirements Specification, 1984

IEEE STD 1012, Institute of Electrical and Electronics Engineers, Inc., Standard for Software Verification and Validation Plans, 1987

ISO 12207-1, International Standards Organization, Information Technology-Software, 1994

Joint Software System Safety Committee, "Software System Safety Handbook", December 1999

NASA NSTS 22254, “Methodology for Conduct of NSTS Hazard Analyses,” May 1987.

National Fire Protection Association, “Flammable and Combustible Liquids Code.”

National Fire Protection Association, “Hazardous Chemical Handbook”

National Fire Protection Association, "Properties of Flammable Liquids, Gases and Solids".

National Fire Protection Association, "Fire Protection Handbook."

Nuclear Regulatory Commission NRC, "Safety/Risk Analysis Methodology", April 12, 1993.

Joint Services Computer Resources Management Group, "Software System Safety Handbook: A Technical and Managerial Team Approach", Published on Compact Disc, December 1999.

Society of Automotive Engineers, Aerospace Recommended Practice 4754: "Certification Considerations for Highly Integrated or Complex Aircraft Systems", November 1996.

Society of Automotive Engineers, Aerospace Recommended Practice 4761: "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", December 1996.

System Safety Society: System Safety Analysis Handbook, July 1997.

INDIVIDUAL REFERENCES

Ang, A.H.S., and Tang, W.H., "Probability Concept in Engineering Planning and Design", Vol. II John Wiley and Sons, 1984.

Anderson, D. R., Dennis J. Sweeney, Thomas A. Williams, "An Introduction to Management Science Quantitative Approaches to Decision Making." West Publishing Co., 1976.

Bahr, N. J., "System Safety Engineering and Risk Assessment: A Practical Approach", Taylor and Francis 1997.

Benner, L. "Guide 7: A Guide for Using energy Trace and Barrier Analysis with the STEP Investigation System", Events Analysis, Inc., Oakton, Va., 1985.

Briscoe, G.J., "Risk Management Guide", EG&G Idaho, Inc. SSDC-11, June 1997.

Brown, M., L., "Software Systems Safety and Human Error", Proceedings: COMPASS 1988

Brown, M., L., "What is Software Safety and Who's Fault Is It Anyway?" Proceedings: COMPASS 1987

Brown, M., L., "Applications of Commercially Developed Software in Safety Critical Systems", Proceedings of Parari '99, November 1999

Bozarth, J. D., Software Safety Requirement Derivation and Verification, Hazard Prevention, Q1, 1998

Card, D.N. and Schultz, D.J., "Implementing a Software Safety Program", Proceedings: COMPASS 1987

Clark, R., Benner, L. and White, L. M., "Risk Assessment Techniques Manual," Transportation Safety Institute, March 1987, Oklahoma City, OK.

Clemens, P.L. “A Compendium of Hazard Identification and Evaluation Techniques for System Safety Application,” Hazard Prevention, March/April, 1982.

Cooper, J.A., “Fuzzy-Algebra Uncertainty Analysis,” Journal of Intelligent and Fuzzy Systems, Vol. 2 No. 4 1994.

Connolly, B., “Software Safety Goal Verification Using Fault Tree Techniques: A Critically Ill Patient Monitor Example”, Proceedings: COMPASS 1989

De Santo, B., “A Methodology for Analyzing Avionics Software Safety”, Proceedings: COMPASS 1988

Dunn, R., Ullman, R., “Quality Assurance For Computer Software”, McGraw Hill, 1982

Forrest, M., and McGoldrick, Brendan, “Realistic Attributes of Various Software Safety Methodologies”, Proceedings: 9 Th International System Safety Society, 1989

Hammer, W., R., “Identifying Hazards in Weapon Systems – The Checklist Approach”, Proceedings: Parari ’97, Canberra, Australia

Hammer, Willie, “Occupational Safety Management and Engineering”, 2 Ed., Prentice-Hall, Inc, Englewood Cliffs, NJ, 1981.

Heinrich, H.W., Petersen, D., Roos, N., “Industrial Accident Prevention: A Safety Management Approach”, McGraw-Hill, 5 Th Ed., 1980.

Johnson, W.G., “MORT –The Management Oversight and Risk Tree,” SAN 821-2, U.S. Atomic Energy Commission, 12 February 1973.

Kije, L.T., “Residual Risk,” Rusee Press, 1963.

Kjos, K., “Development of an Expert System for System Safety Analysis”, Proceedings: 8 Th International System Safety Conference, Volume II.

Klir, G.J., Yuan, B., “Fuzzy Sets and Fuzzy logic: Theory and Applications”, Prentice Hall P T R, 1995.

Kroemer, K.H.E., Kroemer, H.J., Kroemer-Elbert, K.E., “Engineering Physiology: Bases of Human Factors/Ergonomics”, 2 Nd. Ed., Van Nostrand Reinhold, 1990.

Lawrence, J.D., “Design Factors for Safety-Critical Software”, NUREG/CR-6294, Lawrence Livermore National Laboratory, November 1994

Lawrence, J.D., “Survey of Industry Methods for Producing Highly Reliable Software”, NUREG/CR-6278, Lawrence Livermore National Laboratory, November 1994.

Leveson, N., G, “SAFEWARE; System Safety and Computers, A Guide to Preventing Accidents and Losses Caused By Technology”, Addison Wesley, 1995

Leveson, N., G., "Software Safety: Why, What, and How, Computing Surveys", Vol. 18, No. 2, June 1986.

Littlewood, B. and Strigini, L., "The Risks of Software", Scientific American, November 1992.

Mattern, S.F. Capt., "Defining Software Requirements for Safety-Critical Functions", Proceedings: 12 Th International System Safety Conference, 1994.

Mills, H., D., "Engineering Discipline for Software Procurement", Proceedings: COMPASS 1987.

Moriarty, Brian and Roland, Harold, E., "System Safety Engineering and Management", Second Edition, John Wiley & Sons, 1990.

Ozkaya, N., Nordin, M. " Fundamentals of Biomechanics: Equilibrium, Motion, and Defermation", Van Nostrand Reinhold, 1991.

Raheja, Dev, G., "Assurance Technologies: Principles and Practices", McGraw-Hill, Inc., 1991.

Rodger, W.P. "Introduction to System Safety Engineering", John Wiley and Sons.

Russo, Leonard, "Identification, Integration, and Tracking of Software System Safety Requirements", Proceedings: 12 Th International System Safety Conference, 1994.

Saaty, T.L., "The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation", 2 Nd., RWS Publications, 1996.

Stephenson, Joe, "System Safety 2000 A Practical Guide for Planning, Managing, and Conducting System Safety Programs", Van Nostrand Reinhold, 1991.

Tarrants, William, E. "The Measurement of Safety Performance", Garland STPM Press, 1980.

OTHER REFERENCES

DEF(AUST) 5679, Army Standardization (ASA), "The Procurement Of Computer-Based Safety Critical Systems", May 1999

UK Ministry of Defense. Interim DEF STAN 00-54: "Requirements for Safety Related Electronic Hardware in Defense Equipment", April 1999.

UK Ministry of Defense. Defense Standard 00-55: "Requirements for Safety Related Software in Defense Equipment", Issue 2, 1997

UK Ministry of Defense. Defense Standard 00-56: "Safety Management Requirements for Defense Systems", Issue 2, 1996

International Electrotechnical Commission, IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", draft 61508-2 Ed 1.0, 1998