References

1. Ackoff, Russell L. (July 1971). Towards a system of systems concepts. *Management Science* 17 (11):661–671.

2. Aeronautica Civil of the Republic of Colombia. AA965 Cali Accident Report. September 1996.

3. Air Force Space Division. *System Safety Handbook for the Acquisition Manager.* SDP 127-1, January 12, 1987.

4. Aircraft Accident Investigation Commission. Aircraft Accident Investigation Report 96–5. Ministry of Transport, Japan, 1996.

5. James G. Andrus. Aircraft Accident Investigation Board Report: U.S. Army UH-60 Black Hawk Helicopters 87-26000 and 88-26060. Department of Defense, July 13, 1994.

6. Angell, Marcia. 2005. *The Truth about the Drug Companies: How They Deceive Us and What to Do about It*. New York: Random House.

7. Anonymous. American Airlines only 75% responsible for 1995 Cali crash. Airline Industry Information, June 15, 2000.

8. Anonymous. USS Scorpion (SSN-589). Wikipedia.

9. Arnold, Richard. *A Qualitative Comparative Analysis of STAMP and SOAM in ATM Occurrence Investigation.* Master's thesis, Lund University, Sweden, June 1990.

10. Ashby, W. R. 1956. *An Introduction to Cybernetics*. London: Chapman and Hall.

11. Ashby, W. R. 1962. Principles of the self-organizing system. In *Principles of Self-Organization*, ed. H. Von Foerster and G. W. Zopf, 255–278. Pergamon.

12. Ayres, Robert U., and Pradeep K. Rohatgi. 1987. Bhopal: Lessons for technological decision-makers. *Technology in Society* 9:19–45.

13. Associated Press. Cali crash case overturned. CBS News, June 16, 1999 (http://www.csbnews.com/stories/1999/06/16/world/main51166.shtml).

14. Bainbridge, Lisanne. 1987. Ironies of automation. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 271–283. New York: John Wiley & Sons.

15. Bachelder, Edward, and Nancy Leveson. Describing and probing complex system behavior: A graphical approach. *Aviation Safety Conference*, Society of Automotive Engineers, Seattle, September 2001.

16. Baciu, Alina, Kathleen R. Stratton, and Sheila P. Burke. 2007. *The Future of Drug Safety: Promoting and Protecting the Health of the Public, Institute of Medicine*. Washington, D.C.: National Academies Press.

17. Baker, James A. (Chair). The Report of the BP U.S. Refineries Independent Safety Review Panel. January 2007.

18. Barstow, David, Laura Dood, James Glanz, Stephanie Saul, and Ian Urbina. Regulators failed to address risk in oil rig fail-safe device. *New York Times*, New York Edition, June 21, 2010, Page Al.

19. Benner, Ludwig, Jr., Accident investigations: Multilinear events sequencing methods. (June 1975). *Journal of Safety Research* 7 (2):67–73.

20. Bernstein, D. A., and P. W. Nash. 2005. *Essentials of Psychology*. Boston: Houghton Mifflin.

21. Bertalanffy, Ludwig. 1969. *General Systems Theory: Foundations*. New York: Braziller.

22. Billings, Charles. 1996. *Aviation Automation: The Search for a Human-Centered Approach*. New York: CRC Press.

23. Bogard, William. 1989. *The Bhopal Tragedy*. Boulder, Colo.: Westview Press.

24. Booten, Richard C., Jr., and Simon Ramo. (July 1984). The development of systems engineering. *IEEE Transactions on Aerospace and Electronic Systems* AES-20 (4):306–309.

25. Brehmer, B. 1992. Dynamic decision making: Human control of complex systems. *Acta Psychologica* 81:211–241.

26. Brookes, Malcolm J. 1982. Human factors in the design and operation of reactor safety systems. In *Accident at Three Mile Island: The Human Dimensions*, ed. David L. Sills, C. P. Wolf, and Vivien B. Shelanski, 155–160. Boulder, Colo.: Westview Press.

27. Brown, Robbie, and Griffin Palmer. Workers on doomed rig voiced concern about safety. *New York Times*, Page Al, July 22, 2010.

28. Bundesstelle für Flugunfalluntersuchung. Investigation Report. German Federal Bureau of Aircraft Accidents Investigation, May 2004.

29. Cameron, R., and A. J. Millard. 1985. *Technology Assessment: A Historical Approach*. Dubuque, IA: Kendall/Hunt.

30. Cantrell, Rear Admiral Walt. (Ret). Personal communication.

31. Carrigan, Geoff, Dave Long, M. L. Cummings, and John Duffer. Human factors analysis of Predator B crash. *Proceedings of AUVSI: Unmanned Systems North America*, San Diego, CA 2008.

32. Carroll, J. S. 1995. Incident reviews in high-hazard industries: Sensemaking and learning under ambiguity and accountability. *Industrial and Environmental Crisis Quarterly* 9:175–197.

33. Carroll, J. S. (November 1998). Organizational learning activities in high-hazard industries: The logics underlying self-analysis. *Journal of Management Studies* 35 (6):699–717.

34. Carroll, John, and Sachi Hatakenaka. Driving organizational change in the midst of crisis. *MIT Sloan Management Review* 42:70–79.

35. Carroll, J. M., and J. R. Olson. 1988. Mental models in human-computer interaction. In *Handbook of Human-Computer Interaction*, ed. M. Helander, 45–65. Amsterdam: Elsevier Science Publishers.

36. Checkland, Peter. 1981. *Systems Thinking, Systems Practice*. New York: John Wiley & Sons.

37. Childs, Charles W. Cosmetic system safety. *Hazard Prevention*, May/June 1979.

38. Chisti, Agnees. 1986. *Dateline Bhopal*. New Delhi: Concept.

39. Conant, R. C., and W. R. Ashby. 1970. Every good regulator of a system must be a model of that system. *International Journal of Systems Science* 1:89–97.

40. Cook, Richard I. Verite, abstraction, and ordinateur systems in the evolution of complex process control. *3rd Annual Symposium on Human Interaction with Complex Systems (HICS '96)*, Dayton Ohio, August 1996.

41. Cook, R. I., S. S. Potter, D. D. Woods, and J. M. McDonald. 1991. Evaluating the human engineering of microprocessor-controlled operating room devices. *Journal of Clinical Monitoring* 7:217–226.

42. Council for Science and Society. 1977. *The Acceptability of Risks (The Logic and Social Dynamics of Fair Decisions and Effective Controls)*. Chichester, UK: Barry Rose Publishers Ltd.

43. Couturier, Matthieu. *A Case Study of Vioxx Using STAMP*. Master's thesis, Technology and Policy Program, Engineering Systems Division, MIT, June 2010.

44. Couturier, Matthieu, Nancy Leveson, Stan Finkelstein, John Thomas, John Carroll, David Weirz, Bruce Psaty, and Meghan Dierks. 2010. Analyzing the Efficacy of Regulatory Reforms after Vioxx Using System Engineering, MIT Technical Report. Engineering Systems Division.

45. Cox, Lauren, and Joseph Brownstein. Aussie civil suit uncovers fake medical journals. ABC News Medical Unit, May 14, 2009.

46. Cutcher-Gershenfeld, Joel. Personal communication.

47. Daouk, Mirna. *A Human-Centered Approach to Developing Safe Systems*. Master's thesis, Aeronautics and Astronautics, MIT, Dec. 2001.

48. Daouk, Mirna, and Nancy Leveson. An approach to human-centered design. *International Workshop on Humana Error, Safety, and System Design (HESSD '01)*, Linchoping, Sweden, June 2001.

49. Dekker, Sidney. 2004. *Ten Questions about Human Error*. New York: CRC Press.

50. Dekker, Sidney. 2006. *The Field Guide to Understanding Human Error*. London: Ashgate.

51. Dekker, Sidney. 2007. *Just Culture: Balancing Safety and Accountability*. London: Ashgate.

52. Dekker, Sidney. *Report on the Flight Crew Human Factors Investigation Conducted for the Dutch Safety Board into the Accident of TK1951, Boeing 737–800 near Amsterdam Schiphol Airport, February 25, 2009*. Lund University, Sweden 2009.

53. Department of Defense. *MIL-STD-882D: Standard Practice for System Safety*. U.S. Department of Defense, January 2000.

54. Department of Employment. 1975. *The Flixborough Disaster: Report of the Court of Inquiry*. London: Her Majesty's Stationery Office.

55. Diemer, Ulli. Contamination: The poisonous legacy of Ontario's environment cutbacks. *Canada Dimension Magazine*, July–August, 2000.

56. Dorner, D. 1987. On the difficulties people have in dealing with complexity. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 97–109. New York: John Wiley & Sons.

57. Dowling, K., R. Bennett, M. Blackwell, T. Graham, S. Gatrall, R. O'Toole, and H. Schempf. A mobile robot system for ground servicing operations on the space shuttle. *Cooperative Intelligent Robots in Space*, SPIE, November, 1992.

58. Dulac, Nicolas. *Empirical Evaluation of Design Principles for Increasing Reviewability of Formal Requirements Specifications through Visualization*. Master's thesis, MIT, August 2003.

59. Dulac, Nicolas. Incorporating safety risk in early system architecture trade studies. *AIAA Journal of Spacecraft and Rockets* 46 (2) (Mar–Apr 2009).

60. Duncan, K. D. 1987. Reflections on fault diagnostic expertise. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 261–269. New York: John Wiley & Sons.

61. Eddy, Paul, Elaine Potter, and Bruce Page. 1976. *Destination Disaster*. New York: Quadrangle/Times Books.

62. Edwards, M. 1981. The design of an accident investigation procedure. *Applied Ergonomics* 12:111–115.

63. Edwards, W. 1962. Dynamic decision theory and probabilistic information processing. *Human Factors* 4:59–73.

64. Ericson, Clif. Software and system safety. *5th Int. System Safety Conference*, Denver, July 1981.

65. Euler, E. E., S. D. Jolly, and H. H. Curtis. 2001. The failures of the Mars climate orbiter and Mars polar lander: A perspective from the people involved. *Guidance and Control*, American Astronautical Society, paper AAS 01-074.

66. Fielder, J. H. 2008. The Vioxx debacle revisited. *Engineering in Medicine and Biology Magazine* 27(4):106–109.

67. Finkelstein, Stan N., and Peter Temin. 2008. *Reasonable Rx: Solving the Drug Price Crisis*. New York: FT Press.

68. Fischoff, B., P. Slovic, and S. Lichtenstein. 1978. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4: 330–344.

69. Ford, Al. Personal communication.

70. Frola, F. R., and C. O. Miller. System safety in aircraft acquisition. Logistics Management Institute, Washington DC, January 1984.

71. Fujita, Y. What shapes operator performance? JAERI Human Factors Meeting, Tokyo, November 1991.

72. Fuller, J. G. (March 1984). Death by robot. *Omni* 6 (6):45–46, 97–102.

73. Government Accountability Office (GAO). 2006. *Drug Safety: Improvement Needed in FDA's Post-market Decision-making and Oversight Process*. Washington, DC: US Government Printing Office.

74. Gehman, Harold (Chair). Columbia accident investigation report. August 2003.

75. Gordon, Sallie E., and Richard T. Gill. 1997. Cognitive task analysis. In *Naturalistic Decision Making*, ed. Caroline E. Zsambok and Gary Klein, 131–140. Mahwah, NJ: Lawrence Erlbaum Associates.

76. Graham, David J. Testimony of David J. Graham, M.D. Senate 9, November 18, 2004.

77. Haddon, William, Jr. 1967. The prevention of accidents. In *Preventive Medicine*, ed. Duncan W. Clark and Brian MacMahon, 591–621. Boston: Little, Brown.

78. Haddon-Cave, Charles. (October 28, 2009). The Nimrod Review. HC 1025. London: Her Majesty's Stationery Office.

79. Hammer, Willie. 1980. *Product Safety Management and Engineering*. Englewood Cliffs, NJ: Prentice-Hall.

80. Harris, Gardiner. U.S. inaction lets look-alike tubes kill patients. *New York Times*, August 20, 2010.

81. Helicopter Accident Analysis Team. 1998. *Final Report*. NASA.

82. Hidden, Anthony. 1990. *Investigation into the Clapham Junction Railway Accident.* London: Her Majesty's Stationery Office.

83. Hill, K. P., J. S. Ross, D. S. Egilman, and H. M. Krumholz. 2009. The ADVANTAGE seeding trial: A review of internal documents. *Annals of Internal Medicine* 149:251–258.

84. Hopkins, Andrew. 1999. *Managing Major Hazards: The Lessons of the Moira Mine Disaster*. Sydney: Allen & Unwin.

85. Howard, Jeffrey. Preserving system safety across the boundary between system integrator and software contractor. *Conference of the Society of Automotive Engineers*, Paper 04AD-114, SAE, 2004.

86. Howard, Jeffrey, and Grady Lee. 2005. *SpecTRM-Tutorial*. Seattle: Safeware Engineering Corporation.

87. Ingerson, Ulf. Personal communication.

88. Ishimatsu, Takuto, Nancy Leveson, John Thomas, Masa Katahira, Yuko Miyamoto, and Haruka Nakao. Modeling and hazard analysis using STPA. *Conference of the International Association for the Advancement of Space Safety*, IAASS, Huntsville, May 2010.

89. Ito, Shuichiro Daniel. *Assuring Safety in High-Speed Magnetically Levitated (Maglev) Systems*. Master's thesis, MIT, May 2008.

90. Jaffe, M. S. *Completeness, Robustness, and Safety of Real-Time Requirements Specification*. Ph.D. Dissertation, University of California, Irvine, 1988.

91. Jaffe, M. S., N. G. Leveson, M. P. E. Heimdahl, and B. E. Melhart. (March 1991). Software requirements analysis for real-time process-control systems. *IEEE Transactions on Software Engineering* SE-17 (3):241–258.

92. Johannsen, G., J. E. Rijndorp, and H. Tamura. 1986. Matching user needs and technologies of displays and graphics. In *Analysis, Design, and Evaluation of Man–Machine Systems*, ed. G. Mancini, G. Johannsen, and L. Martensson, 51–61. New York: Pergamon Press.

93. Johnson, William G. 1980. *MORT Safety Assurance System*. New York: Marcel Dekker.

94. Joyce, Jeffrey. Personal communication.

95. JPL Special Review Board. Report on the loss of the Mars polar lander and deep space 2 missions. NASA Jet Propulsion Laboratory, 22 March 2000.

96. Juechter, J. S. Guarding: The keystone of system safety. *Proc. of the Fifth International Conference of the System Safety Society*, VB-1–VB-21, July 1981.

97. Kahneman, D., P. Slovic, and A. Tversky. 1982. *Judgment under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.

98. Kemeny, John G. 1979. *Report of the President's Commission on Three Mile Island (The Need for Change: The Legacy of TMI)*. Washington, DC: U.S. Government Accounting Office.

99. Kemeny, John G. 1980. Saving American democracy: The lessons of Three Mile Island. *Technology Review* (June–July):65–75.

100. Kjellen, Urban. 1982. An evaluation of safety information systems at six medium-sized and large firms. *Journal of Occupational Accidents* 3:273–288.

101. Kjellen, Urban. 1987. Deviations and the feedback control of accidents. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 143–156. New York: John Wiley & Sons.

102. Klein, Gary A., Judith Orasano, R. Calderwood, and Caroline E. Zsambok, eds. 1993. *Decision Making in Action: Models and Methods*. New York: Ablex Publishers.

103. Kletz, Trevor. Human problems with computer control. *Plant/Operations Progress* 1 (4), October 1982.

104. Koppel, Ross, Joshua Metlay, Abigail Cohen, Brian Abaluck, Russell Localio, Stephen Kimmel, and Brian Strom. (March 9, 2003). The role of computerized physical order entry systems in facilitating medication errors. *Journal of the American Medical Association* 293 (10):1197–1203.

105. Kraft, Christopher. Report of the Space Shuttle Management Independent Review. NASA, February 1995.

106. Ladd, John. Bhopal: An essay on moral responsibility and civic virtue. Department of Philosophy, Brown University, Rhode Island, January 1987.

107. La Porte, Todd R., and Paula Consolini. 1991. Working in practice but not in theory: Theoretical challenges of high-reliability organizations. *Journal of Public Administration: Research and Theory* 1:19–47.

108. Laracy, Joseph R. *A Systems-Theoretic Security Model for Large Scale, Complex Systems Applied to the U.S. Air Transportation System*. Master's thesis, Engineering Systems Division, MIT, 2007.

109. Lederer, Jerome. 1986. How far have we come? A look back at the leading edge of system safety eighteen years ago. *Hazard Prevention* (May/June):8–10.

110. Lees, Frank P. 1980. *Loss Prevention in the Process Industries, Vol. 1 and 2*. London: Butterworth.

111. Leplat, Jacques. 1987. Accidents and incidents production: Methods of analysis. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 133–142. New York: John Wiley & Sons.

112. Leplat, Jacques. 1987. Occupational accident research and systems approach. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 181–191. New York: John Wiley & Sons.

113. Leplat, Jacques. 1987. Some observations on error analysis. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 311–316. New York: John Wiley & Sons.

114. Leveson, Nancy G. High-pressure steam engines and computer software. *IEEE Computer*, October 1994 (Keynote Address from IEEE/ACM International Conference on Software Engineering, 1992, Melbourne, Australia).

115. Leveson, Nancy G. 1995. *Safeware: System Safety and Computers*. Boston: Addison Wesley.

116. Leveson, Nancy G. The role of software in spacecraft accidents. *AIAA Journal of Spacecraft and Rockets* 41 (4) (July 2004).

117. Leveson, Nancy G. 2007. Technical and managerial factors in the NASA Challenger and Columbia losses: Looking forward to the future. In *Controversies in Science and Technology, Vol. 2: From Chromosomes to the Cosmos*, ed. D. L. Kleinman, K. Hansen, C. Matta, and J. Handelsman, 237–261. New Rochelle, NY: Mary Ann Liebert, Inc.

118. Leveson, Nancy G., Margaret Stringfellow, and John Thomas. Systems Approach to Accident Analysis. IT Technical Report, 2009.

119. Leveson, Nancy, and Kathryn Weiss. Making embedded software reuse practical and safe. *Foundations of Software Engineering*, Newport Beach, Nov. 2004.

120. Leveson, Nancy G. (January 2000). Leveson intent specifications: An approach to building human-centered specifications. *IEEE Transactions on Software Engineering* SE-26 (1):15–35.

121. Leveson, Nancy, and Jon Reese. TCAS intent specification. http://sunnyday.mit.edu/papers/tcas-intent.pdf.

122. Leveson, Nancy, Maxime de Villepin, Mirna Daouk, John Bellingham, Jayakanth Srinivasan, Natasha Neogi, Ed Bacheldor, Nadine Pilon, and Geraldine Flynn. A safety and human-centered approach to developing new air traffic management tools. *4th International Seminar or Air Traffic Management Research and Development*, Santa Fe, New Mexico, December 2001.

123. Leveson, N.G., M. P.E. Heimdahl, H. Hildreth, and J.D. Reese. Requirements specification for process-control systems. *Trans. on Software Engineering*, SE-20(9), September 1994.

124. Leveson, Nancy G., Nicolas Dulac, Karen Marais, and John Carroll. (February/March 2009). Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Organization Studies* 30:227–249.

125. Leveson, Nancy, Nicolas Dulac, Betty Barrett, John Carroll, Joel Cutcher-Gershenfield, and Stephen Friedenthal. 2005. *Risk Analysis of NASA Independent Technical Authority. ESD Technical Report Series, Engineering Systems Division*. Cambridge, MA: MIT.

126. Levitt, R. E., and H. W. Parker. 1976. Reducing construction accidents—Top management's role. *Journal of the Construction Division* 102 (CO3):465–478.

127. Lihou, David A. 1990. Management styles—The effects of loss prevention. In *Safety and Loss Prevention in the Chemical and Oil Processing Industries*, ed. C. B. Ching, 147–156. Rugby, UK: Institution of Chemical Engineers.

128. London, E. S. 1982. Operational safety. In *High Risk Safety Technology*, ed. A. E. Green, 111–127. New York: John Wiley & Sons.

129. Lucas, D. A. 1987. Mental models and new technology. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 321–325. New York: John Wiley & Sons.

130. Lutz, Robyn R. Analyzing software requirements errors in safety-critical, embedded systems. *Proceedings of the International Conference on Software Requirements*, IEEE, January 1992.

131. Machol, Robert E. (May 1975). The Titanic coincidence. *Interfaces* 5 (5):53–54.

132. Mackall, Dale A. Development and Flight Test Experiences with a Flight-Critical Digital Control System. NASA Technical Paper 2857, National Aeronautics and Space Administration, Dryden Flight Research Facility, November 1988.

133. Main Commission Aircraft Accident Investigation Warsaw. Report on the Accident to Airbus A320-211 Aircraft in Warsaw, September 1993.

134. Martin, John S. 2006. Report of the Honorable John S. Martin to the Special Committee of the Board of Directors of Merck & Company, Inc, Concerning the Conduct of Senior Management in the Development and Marketing of Vioxx., Debevoise & Plimpton LLP, September 2006.

135. Martin, Mike W., and Roland Schinzinger. 1989. *Ethics in Engineering*. New York: McGraw-Hill.

136. McCurdy, H. 1994. *Inside NASA: High Technology and Organizational Change in the U.S. Space Program*. Baltimore: Johns Hopkins University Press.

137. Miles, Ralph F., Jr. 1973. Introduction. In *Systems Concepts: Lectures on Contemporary Approaches to Systems*, ed. Ralph F. Miles, Jr., 1–12. New York: John F. Wiley & Sons.

138. Miller, C. O. 1985. A comparison of military and civil approaches to aviation system safety. *Hazard Prevention* (May/June):29–34.

139. Morgan, Gareth. 1986. *Images of Organizations*. New York: Sage Publications.

140. Mostrous, Alexi. Electronic medical records not seen as a cure-all: As White House pushes expansion, critics cite errors, drop-off in care. *Washington Post*, Sunday Oct. 25, 2009.

141. NASA Aviation Safety Reporting System Staff. Human factors associated with altitude alert systems. NASA ASRS Sixth Quarterly Report, NASA TM-78511, July 1978.

142. Nelson, Paul S. *A STAMP Analysis of the LEX Comair 5191 Accident.* Master's thesis, Lund University, Sweden, June 2008.

143. Norman, Donald A. 1990. The "problem" with automation: Inappropriate feedback and interaction, not "over-automation." In *Human Factors in Hazardous Situations*, ed. D. E. Broadbent, J. Reason, and A. Baddeley, 137–145. Oxford: Clarendon Press.

144. Norman, Donald A. (January 1981). Categorization of action slips. *Psychological Review* 88 (1):1–15.

145. Norman, Donald A. (April 1983). Design rules based on analyses of human error. *Communications of the ACM* 26 (4):254–258.

146. Norman, D. A. 1993. *Things That Make Us Smart*. New York: Addison-Wesley.

147. O'Connor, Dennis R. 2002. *Report of the Walkerton Inquiry*. Toronto: Ontario Ministry of the Attorney General.

148. Okie, Susan. 2005. What ails the FDA? *New England Journal of Medicine* 352 (11):1063–1066.

149. Orisanu, J., J. Martin, and J. Davison. 2007. Cognitive and contextual factors in aviation accidents: Decision errors. In *Applications of Naturalistic Decision Making*, ed. E. Salas and G. Klein, 209–225. Mahwah, NJ: Lawrence Erlbaum Associates.

150. Ota, Daniel Shuichiro. *Assuring Safety in High-Speed Magnetically Levitated (Maglev) Systems: The Need for a System Safety Approach*. Master's thesis, MIT, May 2008.

151. Owens, Brandon, Margaret Stringfellow, Nicolas Dulac, Nancy Leveson, Michel Ingham, and Kathryn Weiss. Application of a safety-driven design methodology to an outer planet exploration mission. *2008 IEEE Aerospace Conference*, Big Sky, Montana, March 2008.

152. Pate-Cornell, Elisabeth. (November 30, 1990). Organizational aspects of engineering system safety: The case of offshore platforms. *Science* 250:1210–1217.

153. Pavlovich, J. G. 1999. *Formal Report of the Investigation of the 30 April 1999 Titan IV B/Centaur TC-14/Milstar-3 (B32)*. U.S. Air Force.

154. Pereira, Steven J., Grady Lee, and Jeffrey Howard. A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system. *AIAA Missile Sciences Conference*, Monterey, CA, Nov. 2006.

155. Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technology*. Princeton, NJ: Princeton University Press.

156. Perrow, Charles. 1986. The habit of courting disaster. *The Nation* (October):346–356.

157. Petersen, Dan. 1971. *Techniques of Safety Management*. New York: McGraw-Hill.

158. Pickering, William H. 1973. Systems engineering at the Jet Propulsion Laboratory. In *Systems Concepts: Lectures on Contemporary Approaches to Systems*, ed. Ralph F. Miles, Jr., 125–150. New York: John F. Wiley & Sons.

159. Piper, Joan L. 2001. *Chain of Events: The Government Cover-Up of the Black Hawk Incident and the Friendly Fire Death of Lt. Laura Piper*. London: Brasseys.

160. Psaty, Bruce, and Richard A. Kronmal. (April 16, 2008). Reporting mortality findings in trials of rofecoxib for Alzheimer disease or cognitive impairment: A case study based on documents from rofecoxib litigation. *Journal of the American Medical Association* 299 (15):1813.

161. Ramo, Simon. 1973. The systems approach. In *Systems Concepts: Lectures on Contemporary Approaches to Systems*, ed. Ralph F. Miles, Jr., 13–32. New York: John Wiley & Sons.

162. Rasmussen, Jens. Approaches to the control of the effects of human error on chemical plant safety. In *International Symposium on Preventing Major Chemical Accidents*, American Inst. of Chemical Engineers, February 1987.

163. Rasmussen, J. (March/April 1985). The role of hierarchical knowledge representation in decision making and system management. *IEEE Transactions on Systems, Man, and Cybernetics* SMC-15 (2):234–243.

164. Rasmussen, J. 1986. *Information Processing and Human–Machine Interaction: An Approach to Cognitive Engineering*. Amsterdam: North Holland.

165. Rasmussen, J. 1990. Mental models and the control of action in complex environments. In *Mental Models and Human–Computer Interaction*, ed. D. Ackermann and M. J. Tauber, 41–69. Amsterdam: North-Holland.

166. Rasmussen, Jens. 1990. Human error and the problem of causality in analysis of accidents. In *Human Factors in Hazardous Situations*, ed. D. E. Broadbent, J. Reason, and A. Baddeley, 1–12. Oxford: Clarendon Press.

167. Rasmussen, Jens. Risk management in a dynamic society: A modelling problem. *Safety Science* 27 (2/3) (1997):183–213.

168. Rasmussen, Jens, Keith Duncan, and Jacques Leplat. 1987. *New Technology and Human Error*. New York: John Wiley & Sons.

169. Rasmussen, Jens, Annelise Mark Pejtersen, and L. P. Goodstein. 1994. *Cognitive System Engineering*. New York: John Wiley & Sons.

170. Rasmussen, Jens, and Annelise Mark Pejtersen. 1995. Virtual ecology of work. In *An Ecological Approach to Human Machine Systems I: A Global Perspective*, ed. J. M. Flach, P. A. Hancock, K. Caird, and K. J. Vicente, 121–156. Hillsdale, NJ: Erlbaum.

171. Rasmussen, Jens, and Inge Svedung. 2000. *Proactive Risk Management in a Dynamic Society*. Stockholm: Swedish Rescue Services Agency.

172. Reason, James. 1990. *Human Error*. New York: Cambridge University Press.

173. Reason, James. 1997. *Managing the Risks of Organizational Accidents*. London: Ashgate.

174. Risk Management Pro. Citichem Syndicate: Introduction to the Transcription of the Accident Scenario, ABC Circle Films, shown on ABC television, March 2, 1986.

175. Roberts, Karlene. 1990. Managing high reliability organizations. *California Management Review* 32 (4):101–114.

176. Rochlin, Gene, Todd LaPorte, and Karlene Roberts. The self-designing high reliability organization. *Naval War College Review* 40 (4):76–91, 1987.

177. Rodriguez, M., M. Katahira, M. de Villepin, and N. G. Leveson. Identifying mode confusion potential in software design. *Digital Aviation Systems Conference*, Philadelphia, October 2000.

178. Rubin, Rita. How did the Vioxx debacle happen? *USA Today*, October 12, 2004.

179. Russell, Bertrand. 1985. *Authority and the Individual*. 2nd ed. London: Routledge.

180. Sagan, Scott. 1995. *The Limits of Safety*. Princeton, NJ: Princeton University Press.

181. Sarter, Nadine, and David Woods. (November 1995). How in the world did I ever get into that mode? Mode error and awareness in supervisory control. *Human Factors* 37 (1):5–19.

182. Sarter, Nadine N., and David Woods. Strong, silent, and out-of-the-loop. CSEL Report 95-TR-01, Ohio State University, February 1995.

183. Sarter, Nadine, David D. Woods, and Charles E. Billings. 1997. Automation surprises. In *Handbook of Human Factors and Ergonomics*, 2nd ed., ed. G. Salvendy, 1926–1943. New York: Wiley.

184. Schein, Edgar. 1986. *Organizational Culture and Leadership*. 2nd ed. New York: Sage Publications.

185. Senge, Peter M. 1990. *The Fifth Discipline: The Art and Practice of Learning Organizations*. New York: Doubleday Currency.

186. Shappell, S., and D. Wiegmann. The Human Factors Analysis and Classification System—HFACS. Civil Aeromedical Medical Institute, Oklahoma City, OK, Office of Aviation Medicine Technical Report COT/FAA/AN-00/7, 2000.

187. Sheen, Barry. 1987. *Herald of Free Enterprise Report Marine Accident Investigation Branch, Department of Transport (originally Report of Court No 8074 Formal Investigation)*. London: HMSO.

188. Shein, Edgar. 2004. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.

189. Shockley-Zabalek, P. 2002. *Fundamentals of Organizational Communication*. Boston: Allyn & Bacon.

190. Smith, Sheila Weiss. 2007. Sidelining safety—The FDA's inadequate response to the IOM. *New England Journal of Medicine* 357 (10):960–963.

191. Snook, Scott A. 2002. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq*. Princeton, NJ: Princeton University Press.

192. Staff, Spectrum. 1987. Too much, too soon. *IEEE Spectrum* (June):51–55.

193. Stephenson, A. Mars Climate Orbiter: Mishap Investigation Board Report. NASA, November 10, 1999.

194. Sterman, John D. 2000. *Business Dynamics*. New York: McGraw-Hill.

195. Stringfellow, Margaret. *Human and Organizational Factors in Accidents*. Ph.D. Dissertation, Aeronautics and Astronautics, MIT, 2010.

196. Swaanenburg, H. A. C., H. J. Swaga, and F. Duijnhouwer. 1989. The evaluation of VDU-based man-machine interfaces in process industry. In *Analysis, Design, and Evaluation of Man-Machine Systems*, ed. J. Ranta, 71–76. New York: Pergamon Press.

197. Taylor, Donald H. 1987. The role of human action in man-machine system errors. In *New Technology and Human Error*, ed. Jens Rasmussen, Keith Duncan, and Jacques Leplat, 287–292. New York: John Wiley & Sons.

198. Taylor, J. R. 1982. An integrated approach to the treatment of design and specification errors in electronic systems and software. In *Electronic Components and Systems*, ed. E. Lauger and J. Moltoft, 87–93. Amsterdam: North Holland.

199. Thomas, John, and Nancy Leveson. 2010. *Analyzing Human Behavior in Accidents*. MIT Research Report, Engineering Systems Division.

199a. Thomas, John and Nancy Leveson. 2011. Performing hazard analysis on complex software and human-intensive systems. In *Proceedings of the International System Safety Society Conference*, Las Vegas.

200. U.S. Government Accounting Office, Office of Special Investigations. 1997. *Operation Provide Comfort: Review of Air Force Investigation of Black Hawk Fratricide Incident (GAO/T-OSI-98–13)*. Washington, DC: U.S. Government Printing Office.

201. Vicente, Kim J. 1995. *A Field Study of Operator Cognitive Monitoring at Pickering Nuclear Generating Station. Technical Report CEL 9504, Cognitive Engineering Laboratory*. University of Toronto.

202. Vicente, Kim J. 1999. *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. Mahwah, NJ: Lawrence Erlbaum Associates.

203. Vicente, Kim J., and J. Rasmussen. Ecological interface design: Theoretical foundations. *IEEE Trams. on Systems, Man, and Cybernetics* 22 (4) (July/August 1992).

204. Watt, Kenneth E.F. 1974. *The Titanic Effect*. Stamford, CT: Sinauer Associates.

205. Weick, Karl E. 1987. Organizational culture as a source of high reliability. *California Management Review* 29 (2):112–127.

206. Weick, Karl E. 1999. K. Sutcliffe, and D. Obstfeld. Organizing for high reliability. *Research in Organizational Behavior* 21:81–123.

207. Weinberg, Gerald. 1975. *An Introduction to General Systems Thinking*. New York: John Wiley & Sons.

208. Weiner, E.L. *Human Factors of Advanced Technology ("Glass Cockpit") Transport Aircraft*. NASA Contractor Report 177528, NASA Ames Research Center, June 1989.

209. Weiner, Earl L., and Renwick E. Curry. 1980. Flight-deck automation: Promises and problems. *Ergonomics* 23 (10):995–1011.

210. Wiener, Norbert. 1965. *Cybernetics: or the Control and Communication in the Animal and the Machine*. 2nd ed. Cambridge, MA: MIT Press.

211. Weiss, Kathryn A. *Building a Reusable Spacecraft Architecture Using Component-Based System Engineering*. Master's thesis, MIT, August 2003.

212. Wong, Brian. *A STAMP Model of the Überlingen Aircraft Collision Accident*. S.M. thesis, Aeronautics and Astronautics, MIT, 2004.

213. Woods, David D. Some results on operator performance in emergency events. In *Ergonomic Problems in Process Operations*, ed. D. Whitfield, Institute of Chemical Engineering Symposium, Ser. 90, 1984.

214. Woods, David D. Lessons from beyond human error: Designing for resilience in the face of change and surprise. Design for Safety Workshop, NASA Ames Research Center, October 8–10, 2000.

215. Young, Thomas (Chairman). Mars Program Independent Assessment Team Report. NASA, March 2000.

216. Young, T. Cuyler. 1975. Pollution begins in prehistory: The problem is people. *Man in Nature: Historical Perspectives on Mara in His Environment*, ed. Louis D. Levine. Toronto: Royal Ontario Museum.

217. Zsambok, Caroline E., and Gary Klein, eds. 1997. *Naturalistic Decision Making*. Mahwah, NJ: Lawrence Erlbaum Associates.

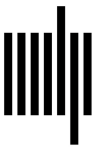
Engineering a Safer World

Systems Thinking Applied to Safety

By: Nancy G. Leveson

Citation:

Engineering a Safer World: Systems Thinking Applied to Safety
By: Nancy G. Leveson
DOI: 10.7551/mitpress/8179.001.0001
ISBN (electronic): 9780262298247
Publisher: The MIT Press
Published: 2016



The MIT Press

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Syntax and Times Roman by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Leveson, Nancy.
Engineering a safer world : systems thinking applied to safety / Nancy G. Leveson.
p. cm.—(Engineering systems)
Includes bibliographical references and index.
ISBN 978-0-262-01662-9 (hardcover : alk. paper)
1. Industrial safety. 2. System safety. I. Title.
T55.L466 2012
620.8′6—dc23
2011014046

10 9 8 7 6 5 4 3 2 1