A Survey of NASA and Military Standards on Fault Tolerance and Reliability Applied to Robotics

Joseph R. Cavallaro and Ian D. Walker
cavallar@rice.edu ianw@rice.edu
Dept. of Electrical and Computer Engineering
Rice University, Houston, TX 77251

Abstract

There is currently increasing interest and activity in the area of reliability and fault tolerance for robotics. This paper discusses the application of Standards in robot reliability, and surveys the literature of relevant existing standards. A bibliography of relevant Military and NASA standards for reliability and fault tolerance is included.

1 Introduction

Applications of intelligent robots are expanding to remote and hazardous environments, such as nuclear waste handling, and undersea and space operations. Fault tolerance and reliability are of paramount importance in these environments, since repair is often difficult, and failures potentially catastrophic.

However, efforts in robot reliability and fault tolerance have often been piecemeal and application-specific. The formality and consistency across applications of Standards and Protocols are successfully applied to many other engineering areas.

The Standards documentation spans several different categories. There are Handbooks (Reliability of Electronic Equipment [7], MIL-HDBK-217F, Fault Tree Handbook [25], NUREG-0492), Parts Specifications and Standards (Aircraft Data Bus [13], MIL-STD-1553B, Aircraft 28V DC Motors [10], MIL-M-8609B) Procedures and Programs (Failure Modes, Effects Analysis [14], MIL-STD-1629A, System Safety Program [20], MIL-STD-882), and Data Item Descriptions (Format for reports required under procedures FMEA [2], for example DI-R-7085A).

Standards utilization varies widely (Reliability Data in MIL-HDBK-217F covers a variety of components under thermal stress, some Standards include handbooks on failure data for electronic equipment, an Aircraft Survivability Program Standard [16], MIL-STD-2072, references documents from the Defense Nuclear Agency on Nuclear Weapon Effects on Aircraft). However, most Standards deal with non-nuclear environments, and further studies are needed for hazardous waste sites. There are also Standards for Software Quality [3], for example DOD-STD-2168.

This paper will discuss the potential application and tailoring for robotics applications of the existing standards, including the Robotic Industries Association (RIA) and American National Standard for Industrial Robots and Robot Systems standards. A standard has been developed for safety requirements [28], ANSI/RIA R15.06-1986 and a new standard is proposed for reliability [27], BSR/RIA R15.05-3-199X. For example, procedures for a failure modes and effects analysis (FMEA) described in standard MIL-STD-1629A, together with DI-R-7085A, allow tailoring of the speci-

[0]Copyright ©1994 by the American Institute of Aeronautics and Astronautics, Inc. All rights reserved.

fications to the robot needs. We will note the use of FMEA in robot system reliability [1], together with ongoing work in architectures for robot fault detection and fault tolerance [30].

2 Standards Categories

The military standards literature can be divided into a number of major categories [26, 31]. These include handbooks and parts specifications useful in the characterization of components for a system. Other documents describe procedures and programs which are useful for design, analysis, or system operation. Additionally, data item description documents provide standardized report generation procedures which are useful for system specification and procurement.

2.1 Handbooks

One of the more widely used military standards handbooks is MIL-HDBK-217F, Reliability of Electronic Equipment [7]. This handbook provides tables to calculate failure rates for a number of electronic components from resistors and capacitors, to switches and relays, to motors and resolvers. Reliability data for mundane components, such as connectors, is presented along with failure estimates for complex integrated circuits, such as microprocessors. The failure rates are also based on the environment in which the component is expected to be used from benign ground use to extreme missile or cannon launch. Thermal effects on component reliability are considered very important in the derating analysis.

NASA has published a standard for reliability [24], NASA-TM-4322 which references the data in MIL-HDBK-217F. In the NASA document, tables are given which further derate components for space use beyond the factors given in MIL-HDBK-217F. Examples of failure rate calculations are given in section 3.

The use of MIL-HDBK-217F is described in a tutorial handbook, MIL-HDBK-338-1A, Electronic Reliability Design Handbook [8]. A valuable handbook for system reliability analysis is published by the Nuclear Regulatory Commission as NUREG-0492, the Fault Tree Handbook [25].

2.2 Parts Specifications

In addition to the more generic handbooks, there is a large collection of standards for individual parts. Many of the standards were developed for a particular military project which required a specific design. Many of the standards for aircraft components may be useful for specifying the reliability of robotic assemblies. Electric motors [10] are described in MIL-M-8609B while hydraulic actuators are described in MIL-A-5503E [5] and MIL-M-7997C [9]. The bibliography lists other standards for components such as shaft encoders and various switches which could be used as limit switches. As an example, the standard for an aircraft computer data bus, MIL-STD-1553B [13] was used in the design specification of the NASA Flight Telerobotic Servicer (FTS) project [22].

2.3 Procedures and Programs

When a particular system is in the design phase, it is useful to perform a failure modes and effects analysis. Tools such as fault trees may be used to generate this analysis. In addition, the analysis needs to be customized for the system and its intended use. In MIL-STD-1629A, a procedure for a generic Failure Modes and Effects Analysis [14] is given. For systems that may cause harm to people or other equipment, a safety protocol should be developed. In MIL-STD-882, a System Safety Program [20] which identifies hazards is described.

2.4 Data Item Descriptions

Data item descriptions describe the format for reports required under various procedures. For example, reports generated for a failure modes and effects analysis of a system would be written in a format given [2] by DI-R-7085A. NASA has similar doucmentation formats such as the

NASA Assurance Specification Documentation Standard [23], NASA-TM-101859. These format specifications are valuable in generating design, operation and maintenance documents.

3 Failure Probability

As detailed in [1, 25], the probability of a component failure can be calculated from a failure rate for the component [4]. Given a constant failure rate λ and using the exponential distribution, the probability of failure at time t is [1]:

$$p(t) = 1 - e^{-\lambda t},$$

the reliability of the component in the system is given by

$$R(t) = 1 - p(t) = e^{-\lambda t},$$

and the mean time to failure (MTTF) is given as

$$MTTF = 1/\lambda.$$

If the failure rate is small, the probability of failure is often approximated as λt [25]. An expert system can be used to model component decay by using time-dependent probabilities [25]. A small update routine monitors the system time and modifies the basic probability facts during the life of the robot.

Various methods can be used to determine the failure rate λ. For example, in [7], the average failure rate λ_m for a D.C. motor is estimated as

$$\lambda_m = [(t^2/\alpha_B^3) + (1/\alpha_W)]$$

failures per 10^6 hours, where t is the operating time period for which λ_m is the average failure rate, α_B is the bearing characteristic life, and α_W is the winding characteristic life of the device. Both α_B and α_W depend on the ambient temperature for the device, with expressions given in [7]. For an ambient temperature of $20^o C$, an operating period of 100 hours, the data in [7] gives a failure rate of 6.3×10^{-7} failures per hour.

Also in [7], the average failure rate λ_r for a resolver is given as

$$\lambda_r = \lambda_b \pi_S \pi_N \pi_E$$

failures per 10^6 hours, where λ_b is the base failure rate (exponentially related to ambient temperature), π_S is a factor related to the device size, π_N is related to the number of brushes, and π_E is an environmental factor. For a small resolver with 4 brushes and the same ambient temperature as the motor above in a (possibly mobile) ground-based environment, the failure rate λ_r is found from data in [7] to be 1.6×10^{-6} failures per hour.

The calculation of failure rates is useful to complete a fault tree analysis. Once failure rates have been found for the components, it is possible to compute failure probabilities from this data. Within the fault trees, these failure probabilities are combined through the logic gates using simple multiplication and addition [25]. The probability of failure for the output event of an AND-gate is the product of all the input probabilities and a conservative estimate of the output event probability for an OR-gate is the sum of the input probabilities.

In [29], an expert system is used to maintain the probability of failure for each node within the fault tree. The operator initializes only the basic components (leaves) in the tree with appropriate probability facts. The expert system then initializes the probabilities for inner nodes of the tree by combining the basic component probabilities through the gates in the tree structure. For purposes of design and planning, it is possible to explore the effects of individual component reliability on the overall reliability of the system.

4 Conclusions

Fault tolerance is of increasing concern in the design and use of robots. The military, nuclear power, and space programs have developed a number of reliability standards for the design and analysis of complex systems. The application of these standards to the design of robots will be extremely important in many applications, particularly in hazardous environments. Industrial groups, such as RIA, have proposed standards for safety and are currently developing standards for reliability.

Acknowledgments

This work was supported in part by NSF under grants DDM-9202639 and MSS-9024391 and by DOE Sandia National Laboratory Contract #18-4379A.

References

[1] B.S. Dhillon. *Robot Reliability and Safety.* Springer-Verlag, New York, NY, 1991.

[2] DI-R-7085A. Failure Mode, Effect, and Criticality Analysis Report. Data item description, DOD, September 1984.

[3] DOD-STD-2168. Defense System Software Quality Program. Technical report, DOD, ARDEC, Picatinny Arsenal, NJ, April 1986.

[4] V. H. Guthrie and D. K. Whittle. RAM Analysis Software for Optimization of Servomanipulator Designs. DOE Small Business Innovative Research (SBIR) Program Report JBFA-101-89, JBF Associates, Inc., Knoxville, TN, March 1989. Performed for Oak Ridge National Laboratory.

[5] MIL-A-5503E. Actuators: Aeronautical Linear Utility, Hydraulic, General Specification for. Military specification, DOD, ASD, Wright-Patterson AFB, OH, January 1986.

[6] MIL-E-85082(AS). Encoders, Shaft Angle to Digital, General Specification for. Technical report, DOD-Naval Air Systems, Washington, DC, September 1977.

[7] MIL-HDBK-217F. Reliability Prediction of Electronic Equipment. Technical report, DOD, Rome Laboratory, Griffiss AFB, NY, January 1990.

[8] MIL-HDBK-338-1A. Electronic Reliability Design Handbook. Technical report, DOD, Rome Laboratory, Griffiss AFB, NY, October 1988.

[9] MIL-M-7997C. Motors, Aircraft Hydraulic, Constant Displacement General Specification for. Military specification, DOD, NAEC, Lakehurst, NJ, September 1981.

[10] MIL-M-8609B. Motors, Direct-Current, 28 Volt System, Aircraft General Specification for. Military standard, DOD, December 1987. Notice 1.

[11] MIL-S-8805/57B. Military Specification Sheet Switch, Actuator, Plunger Type. Technical report, DOD, June 1990. Notice 1.

[12] MIL-S-8805/59A. Military Specification Sheet: Switch, Actuator, Roller Leaf. Technical report, DOD, June 1990. Notice 1.

[13] MIL-STD-1553B. Aircraft Internal Time Division Command/Response Multiplex Data Bus. Technical report, DOD, ASD, Wright-Patterson AFB, OH, September 1978.

[14] MIL-STD-1629A. Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Technical report, DOD, NAEC, Lakehurst, NJ, November 1980.

[15] MIL-STD-2069. Requirements for Aircraft Nonnuclear Survivability Program. Technical report, DOD, NAEC, Lakehurst, NJ, August 1981.

[16] MIL-STD-2072. Survivability, Aircraft; Establishment and Conduct of Programs for. Technical report, DOD, Dept. of Navy, Air Systems Command, August 1977.

[17] MIL-STD-781D. Reliability Testing for Engineering Development, Qualification, and Production. Technical report, DOD, October 1986.

[18] MIL-STD-785B. Reliability Program for Systems and Equipment Development and Production. Technical report, DOD, ASD, Wright-Patterson AFB, OH, September 1980.

[19] MIL-STD-810E. Environmental Test Methods and Engineering Guidelines. Technical report, DOD, July 1989.

[20] MIL-STD-882B. System Safety Program Requirements. Technical report, DOD, AFSC, Andrews AFB, Washington, DC, March 1984.

[21] MIL-T-48460B(AR). Military Specification: Tachometer, Rate, Computer: 11732700. Technical report, DOD-Army, ARRADCOM, Dover, NJ, January 1987.

[22] NASA. Computer Based Control System Noncompliance Report for Computer Independent Hazard Control System. REPORT, NASA Goddard Flight Center, Greenbelt, MD, September 1991.

[23] NASA-TM-101859. Assurance Specification Documentation Standard and Data Item Description: Volume of the Information System Life-Cycle and Documentation Standards. Technical Report Technical Memorandum 101859, NASA Office of Safety, Reliability, Maintainability, and Quality Assurance, Washington, DC, February 1989.

[24] NASA-TM-4322. NASA Reliability Preferred Practices for Design and Test. Technical Report Technical Memorandum 4322, NASA Office of Safety and Mission Quality, Washington, DC, April 1991.

[25] NUREG-0492. Fault Tree Handbook. Technical report, Nuclear Regulatory Commission, 1981.

[26] M. Pecht and E. Hakim. The Future of Military Standards: A Focus on Electronics. *IEEE Aerospace and Electronic Systems Magazine*, 7(7):16–19, July 1992.

[27] BSR/RIA R15.05-3-199X. Proposed American National Standard for Industrial Robots and Robot Systems - Guidelines for Reliability Acceptance Testing. Technical report, ANSI/RIA, 1993.

[28] ANSI/RIA R15.06-1986. American National Standard for Industrial Robots and Robot Systems - Safety Requirements. Technical report, ANSI/RIA, 1986.

[29] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker. Expert System Framework of Fault Detection and Fault Tolerance for Robots. In *Robotics and Manufacturing: Recent Trends in Research, Education, and Applications. Proceedings of the Fourth International Symposium on Robotics and Manufacturing*, pages 793–800, Santa Fe, NM, November 1992. ASME Press, New York, NY.

[30] I.D. Walker and J.R. Cavallaro. Dynamic Fault Reconfigurable Intelligent Control Architectures for Robotics. In *Proceedings 1993 Fifth American Nuclear Society Meeting on Robotics and Remote Handling*, pages 305–312, Knoxville, TN, 1993.

[31] G. F. Watson. MIL Reliability: a New Approach. *IEEE Spectrum*, 29(8):46–49, August 1992.