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

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 documentation 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 $\lambda$ 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 $\lambda t$ [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 $\lambda$. For example, in [7], the average failure rate $\lambda_m$ 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 $\lambda_m$ is the average failure rate, $\alpha_B$ is the bearing characteristic life, and $\alpha_W$ is the winding characteristic life of the device. Both $\alpha_B$ and $\alpha_W$ depend on the ambient temperature for the device, with expressions given in [7]. For an ambient temperature of 20°C, an operating period of 100 hours, the data in [7] gives a failure rate of $6.3 \times 10^{-7}$ failures per hour.

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

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

failures per $10^6$ hours, where $\lambda_b$ is the base failure rate (exponentially related to ambient temperature), $\pi_S$ is a factor related to the device size, $\pi_N$ is related to the number of brushes, and $\pi_E$ 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 $\lambda_r$ is found from data in [7] to be $1.6 \times 10^{-6}$ 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


