Proc. 7th American Nuclear Society Topical Meeting on Robotics
and Remote Systems, Vol. 2, pp. 1096-1102, Augusta, GA, April 1997.

Failure Mode Analysis of a Proposed Manipulator-based Hazardous Material Retrieval System

Joseph R. Cavallaro and Ian D. Walker
Rice University
Department of Electrical & Computer Engineering
Houston, TX 77251
E-mail: cavallar@ece.rice.edu, ianw@ece.rice.edu
(713) 527-4020

Abstract

Failure mode and reliability analysis is particularly important for robot manipulators to be deployed in remote environments, where inspection and repair are difficult, and reliability is of prime importance. This is particularly true for manipulators involved in hazardous waste management operations, where failure could be both expensive and highly dangerous. In this paper, we describe a Fault Tree Analysis and detailing of the major failure modes of a robot manipulator-based system for tank waste retrieval. The advantages and limitations of this type of analysis for hazardous waste robotics are detailed and discussed.

1 Introduction

The study of the reliability of robot systems for use in hazardous environments is an important topic that is the subject of much current industrial and academic research.[2,5,8,10,15,18] One of the key steps in the reliability and safety analysis of such robotic systems is the off-line identification and analysis of the potential failure modes within the system under its expected operating conditions. An established technique for this type of failure mode analysis of complex interdisciplinary systems is Fault Tree Analysis.[7,13] The use of Fault Trees, which logically interconnect the effect of (widely disparate) subsystem faults on the overall system, has been shown to be particularly applicable to complex systems such as robot manipulators.[15,16] A fault tree analysis produces a set of interconnected trees modeling a given critical system failure scenario. This is the top event in the overall failure tree. Failure events which could lead to the top event and their interrelations are detailed in the trees. The symbols used in typical fault trees include logical AND gates and OR gates. Essentially, the sequence of events which could lead to the given critical failure scenario are identified and logically combined into a tree structure. For a more detailed description of the fault tree technique, the reader is encouraged to consult.[7,13,14] Other references of interest on related failure mode effect and criticality analysis are contained in several standards.[3,6]

In this paper, a qualitative Fault Tree Analysis and detailing of the major failure modes of the Modified Light Duty Utility Arm (MLDUA) and complementary Hose Management System (HMS), prior to its deployment at Oak Ridge National Laboratory (ORNL) is described. The analysis is based on conceptual design drawings for the MLDUA/HMS system (supplied by ORNL), a Design Report of the Light Duty Utility Arm (LDUA)[9] (supplied by Westinghouse Hanford Company), a design report on the Hose Management Arm (HMA),[1] and on discussions

with ORNL personnel. A conceptual sketch of the MLDUA/HMS system in place over an underground storage tank is shown in Figure 1.

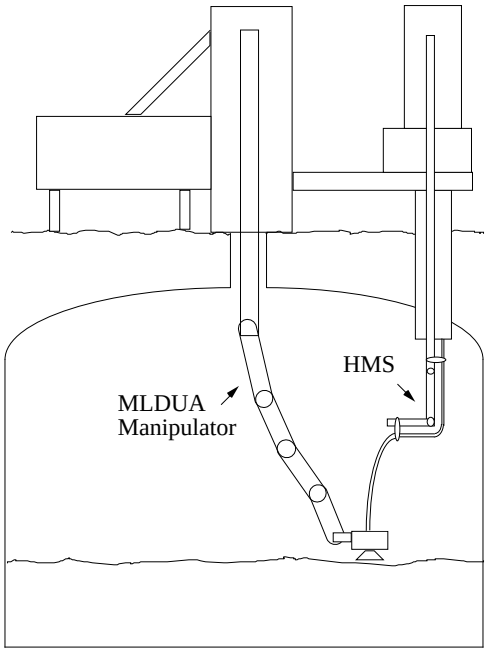

Figure 1: MLDUA and HMS concept.

The following section introduces the MLDUA/HMA system, and describes a fault tree analysis conducted for the system. A summary of the results of and conclusions resulting from the analysis follow, along with a discussion of the applicability of such analyses for hazardous waste robotics.

2 MLDUA/HMS System and its Analysis

The MLDUA/HMS system was scheduled to be deployed in an underground storage tank at Oak Ridge National Laboratory (ORNL) in the fall of 1996. The system was designed to demonstrate the feasibility of robotic removal of tank waste by removing the waste heel of the tank.

The system consists of two major components; (1) an actively controlled robotic arm, the Modified Light Duty Utility Arm (MLDUA); and (2) a specially developed Hose Management System (HMS). Each of these systems has to be lowered into the tank through risers in the roof of the tank. The HMS supports a confined sluicing end-effector and jet pump to dislodge and retrieve the waste. This end-effector is serviced by several high pressure water hoses and a conveyence hose. The end effector of the MLDUA arm is connected to the HMS, and the MLDUA system is used to position and move the HMS systems around the tank.

Safety and reliability are key concerns with the system and demonstration. The authors prepared a report[17] containing a preliminary failure mode analysis and support for the ongoing design and review process for the MLDUA/HMS system. The work, continuing the authors' previous work in fault tree analysis for manipulators[15,16] drew upon resources developed as part of previous contracts with Sandia National Laboratories including access to NASA and DOD documentation and standards. The issues raised in the analysis, which are summarized in this paper, are expected to be typical of those likely to be found in failure mode analyses of robot manipulators

in hazardous waste scenarios.

2.1 Assumptions/Scope

A number of assumptions were made in producing the fault trees. The fundamental (top event) failure event considered is the failure of the robot system to complete its task. This could be due to failure of the MLDUA arm or the HMS system. The task is assumed to include the insertion of the system into the tank, the removal of waste from the tank, and removal of the system from the tank. The top event failure could be the inability to remove the MLDUA arm from the tank, due to failure of the limping mechanism (which allows the robot joints to hang vertically for easy removal of the arm) for example. Alternatively, the top event failure could be due to an in-tank failure of the arm, leading to a seizure, contact, or collision. The types of failure modes considered in the fault trees include, among others, power, sensor, and actuation failures.

The design of the MLDUA robot is assumed to be the same as that of the LDUA design[9] (there are modifications to the MLDUA design from the LDUA, but these are not expected to significantly impact system reliability). Failure modes from cameras or viewing equipment were not considered in the fault trees. The operator is assumed to have access to a monitor with camera feed from inside the tank. The fault trees include failure modes due to software and human errors. These modes were however not expanded due to lack of data on the details of the software configuration and operator interface and protocols.

2.2 Fault Trees

The basic structure of the trees is shown in Figure 2, which gives an indication of the complexity involved. In this example, there are twenty-two views or subtrees, with View 1 being the total fault tree. Only a few of the fault trees from the report[17] are presented in this paper due to space limitations. The main subtree of the system covers faults within the MLDUA itself. Failure modes of the deployment and support structure of the MLDUA are expected to be present in the system, and subtrees covering these failure modes are seen. Fault trees for the actively driven Hose Management Arm form the other major set of subtrees. The set of subtrees or views of the fault tree shown in Figure 2 is listed in Table 1. Figure 3 contains View 2 which is the top event tree, which is the root for all following subtrees. View 3 contains those failure modes of the Mobile Deployment System (MDS) that was expected to form part of the MLDUA/HMS system. Views 4-8 concentrate on the Mast structure of the MLDUA system, and views 10-19 describe the MLDUA itself. Figure 4 presents the top MLDUA fault tree in View 10. Fault trees for the HMS are presented in views 20-22.

The symbols within the dotted circles in the trees label the interconnection of the various subtrees. Each tree is labeled by the symbol in the dotted circle on the right of its top level event box. Labels in dotted circles next to a dotted triangle denote the label of a higher- or lower- level tree to which the current tree is connected, at the connect point.

3 Discussion and Conclusions

Through the fault trees, the major failure modes of the system and their interconnections were identified. The effect of safety systems incorporated into the system are seen (via the AND- gates in the fault trees). In addition, those failure modes from which the system does not have explicit protection (and thus may be the cause of particular concern from a reliability point of view), are highlighted by the fault trees. These failure modes are connected by paths with few or no AND- gates between the failure mode to top event failure (for example, a

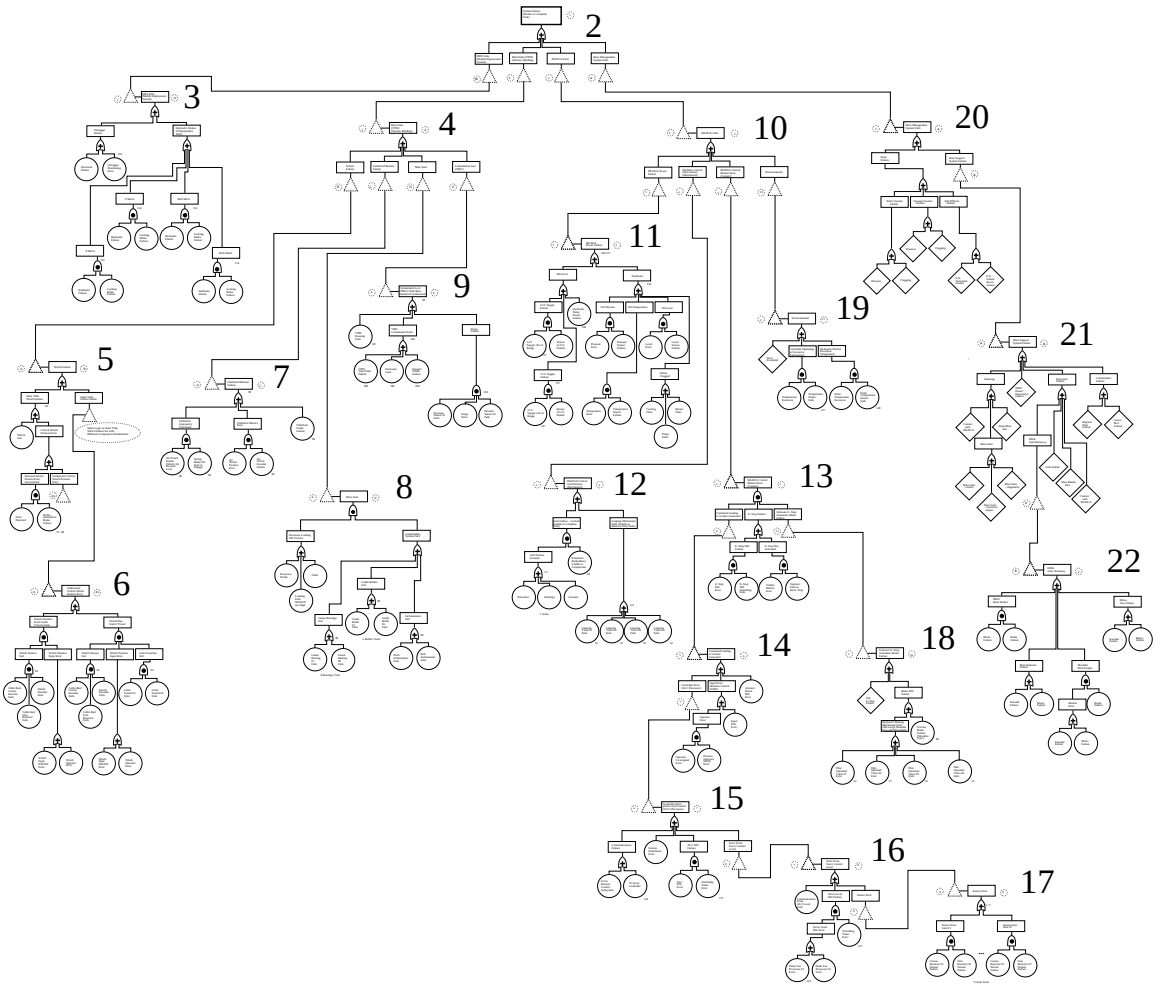

Figure 2: Graphical Fault Tree Organization, View 1

runaway motor failure in the HMA mast rotation joint causes overall system failure, and is an unprotected failure mode). Where these critical failure modes are considered likely to occur, then consideration might be given to the addition of extra redundancy or safety systems to protect the system from these modes.

In general, the fault trees underscored and highlighted the utility of the backup and safety systems incorporated into the MLDUA design. However, there were concerns about some failure modes in the HMA system, and in the actuator systems which were highlighted by the trees. To investigate these issues further, a more detailed fault tree analysis (including a quantitative analysis - see below) could be carried out for the particular failure paths of concern.

The fault trees also confirmed the importance of key sensors (temperature, pressure, joint position, etc.) in the system. Without these sensors, the trees highlight how many simple subsystem faults (for example a hydraulic fluid pressure loss) would very quickly cause a failure of the overall system. For sensors in systems considered especially critical, it may appropriate to perform a more in-depth reliability analysis of the sensors in that system. In the case of the MLDUA system, the analysis was performed after the design phase, and thus adding new sensors was not feasible. In general however, fault tree analyses can also identify areas where the addition of extra sensors would be most beneficial.

Table 1: Fault Tree Organization

Sub-tree Title	View
Total Graphical Fault Tree	1
Top Level Fault Tree - Failure to Complete Task	2
Mobile Deployment System (MDS) Fails	3
Mast Fails (VPM) Seizure, Binding	4
Mast Winch Failure	5
Undetected Critical Mast Winch Position Error	6
Mast Umbilical/Harness Failure	7
Mast Jams	8
Containment Lost Tank Riser Interface/Confinement (TRIC)	9
MLDUA Fails	10
MLDUA Power Failure	11
MLDUA Critical Joint Seizure (Mechanical)	12
MLDUA Critical Motion Error (Contact)	13
MLDUA Command Leading to Contact Generated	14
MLDUA Controller Error - Arm Level Control (ALC) Processor	15
MLDUA Error From Servo Control Level	16
MLDUA Internal Sensor Error	17
MLDUA Software E-Stop / Automatic Brake Failure	18
MLDUA Environmental	19
Hose Management System Failure	20
Hose Support System Failure	21
Hose Management Arm Joint Runaway	22

The trees also highlight the need for, and importance of, effective fault detection strategies in the system. Many of the safety systems highlighted by AND- gates in the fault trees (for example brakes on manipulator joints) will not be effective unless faults which would call them into use are quickly and unambiguously detected. Thus, fault detection will be critical in making use of the safety systems already present in the system, and highlighted by the fault trees.[17] This comment also holds in general for systems where redundancy has been added for system reliability - effective means must be found to ensure that the system selects "healthy" subsystems.

The set of fault trees[17] presented highlight many of the major failure modes in the MLDUA/HMS system, and are felt by the authors to be fairly representative of the type of fault trees required to analyze robot systems in hazardous waste environments. The trees combine, in a straightforward way, failure modes from the various electromechanical and computer hardware subsystems, as well as human operator and software failure modes. This, along with the ability to analyze multiple failures, is a key advantage of fault trees.

However, the trees[17] were synthesized at a fairly high level. The high level nature of some of the trees was due to a lack of available detailed information on the subsystem designs. Given more detailed information on the designs, and of the software and computer control architecture, many of the 'leaves' of the fault trees could have been expanded to provide a more detailed and complete analysis. This is not a major limitation in the case of the MLDUA system, as the trees have been updated as new data has become available. This does however illustrate that the accuracy of any fault tree analysis will always be limited by the fidelity of the information available about the system and its operating environment.

Finally, the fault trees[17] are of a qualitative nature, detailing the logical interactions of the failure modes of the system. No attempt was made to quantify the numerical probabilities of failure of the various subsystems. However, fault trees are inherently designed for quantitative, as well as qualitative, analysis. Given data on the predicted mean time to failure of the various subsystems, the fault trees could also be used in a straightforward fashion to form the core of a numerical reliability analysis of the system. This would help to identify which of the failure paths highlighted as problematic by the qualitative analysis have relatively high probability of occurring.

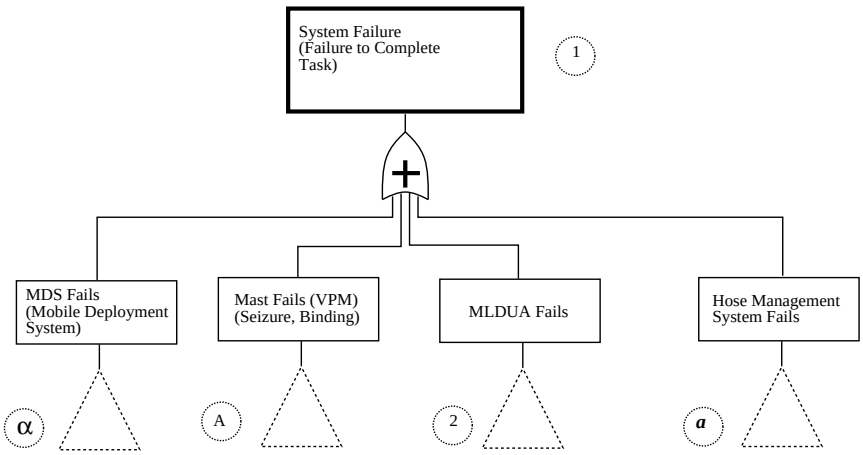

Figure 3: Top Level Fault Tree (View 2) - Failure to Complete Task

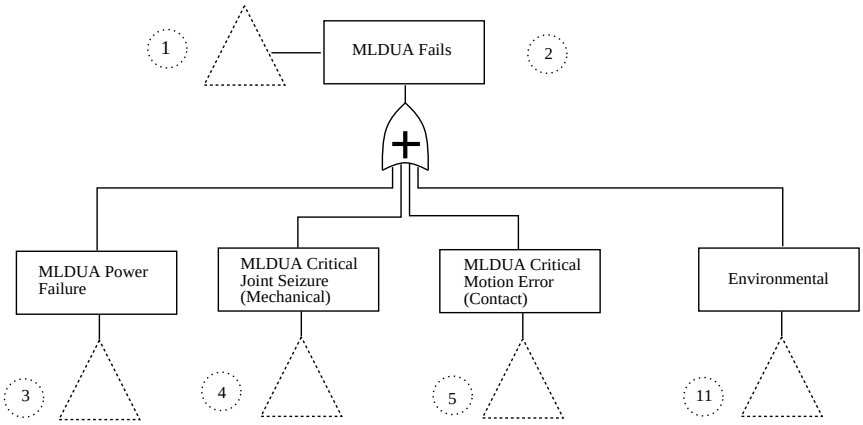

Figure 4: MLDUA Fails (View 10)

In this case however, there is an added difficulty when analyzing robot systems for hazardous waste environments, over the case of more traditional robot applications. Failure rate data is typically not available, or well trusted (for the types of subsystems and components present in robots) for the conditions present in hazardous and/or nuclear environments. In addition, many robot systems designed for these environments are 'one-of-a-kind' (as in the case of the MLDUA system), or 'several-of-a-kind' systems. Thus there is little fault or reliability data available for these systems, even in conventional or test conditions. Thus, quantitative analysis is more difficult, and either data consistent with the hazardous environments must be found, or estimates of failure data and/or approximate methods must be used. There is currently work underway in this regard, both for generation of fault data for robot components under radiation[11,12] and in formal methods for fault tree analysis with uncertain data,[4] which show good promise.

In summary, fault tree analysis appears to be ideally suited for failure mode and reliability analysis of robot manipulators. The analysis of robots for hazardous environments presents several special problems, some of which were highlighted by the analysis of the MLDUA system described in this paper. However, there are several key advantages of fault tree analysis which suggest that it is likely to become and remain a key tool in the reliability and fault tolerance analysis of robots in the future.

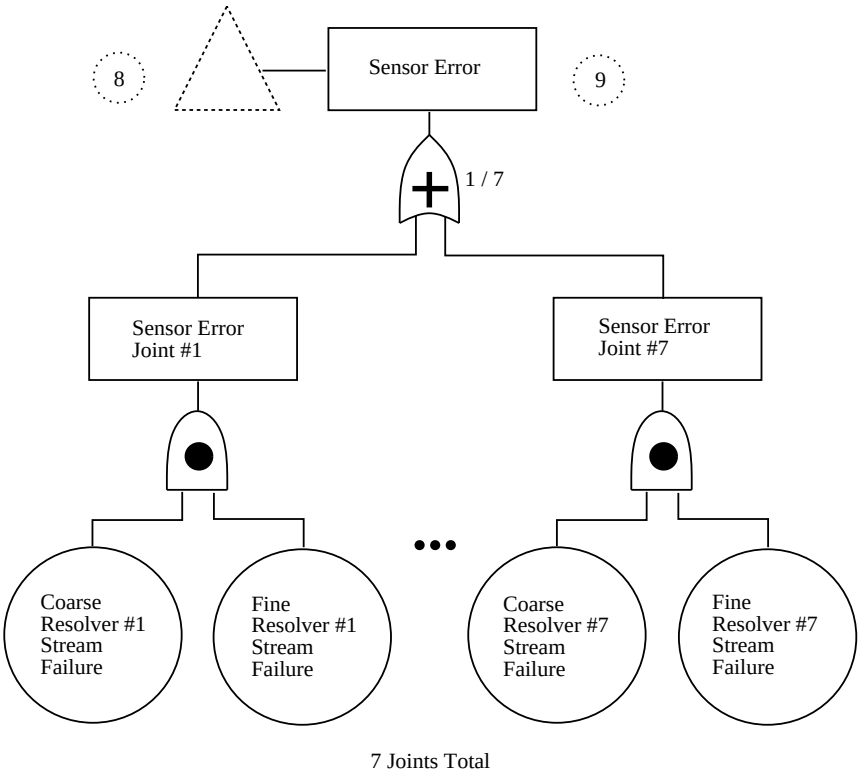

Figure 5: MLDUA Internal Sensor Error (View 17)

Acknowledgments

This work was supported in part by the National Science Foundation under grants IRI-9526363 and DDM-9202639, by DOE Sandia National Laboratory Contract AL-3017, by DOE contract DE-AC04-94AL8500, and NASA contract NAG-9-740.

4 REFERENCES

[1] J. A. Blank. Equipment Specification #ES-GATT-001 for the Waste Dislodgin and Conveyance System of the Gunite and Associated Tanks - Treatability Study. 90% Design Submittal, prepared for: Lockheed Martin Energy Systems, Inc., Oak Ridge, TN, January 1996.

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

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

[4] M. L. Leuschen, I. D. Walker, and J. R. Cavallaro. Robot Reliability Using Fuzzy Fault Trees and Markov Models. In *Proc. SPIE Sensor Fusion and Distributed Robotic Agents*, volume 2905, pages 73–91, Boston, MA, November 1996.

[5] C. Lewis and A.A. Maciejewski. Dexterity Optimization of Kinematically Redundant Manipulators in the Presence of Joint Failures. *International Journal of Computers and Electrical Engineering*, 20(3):273–288, 1994.

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

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

[8] C. Paredis, A. Au, and P. Khosla. Kinematic Design of Fault Tolerant Manipulators. *International Journal of Computers and Electrical Engineering*, 20(3):211–220, 1994.

[9] SPAR. Light Duty Utility Arm LDUA and Deployment System - Detailed Design Report. Document SPAR-LDUA-R.025, prepared for: Westinghouse Hanford Company, Richland, WA, September 1994.

[10] G. Toye and L. Leifer. Helenic Fault Tolerance for Robots. *International Journal of Computers and Electrical Engineering*, 20(6):479–497, 1994.

[11] J. S. Tulenko, D. Ekddahl, L. Utley, and H. Hamilton. On-line Annealing Processes for Hardening Electronic Components in Mobile Robots for Radiation Environments. In *Proceedings of the ANS Conference on Remote Systems Technology*, pages 183–186, San Francisco, CA, 1991.

[12] J.S. Tulenko, D. Ekdahl, H. Liu, K. Phillips, S. Jones, T. Cable, and H. Harvey. Development of a Radiation Resistant ANDROS Robot for Operation in Severe Environments. In *Proceedings American Nuclear Society Topical Meeting on Robotics and Remote Systems*, pages 165–168, Monterey, CA, 1995.

[13] W. E. Vesley, F. F. Goldberg, N. H. Roberts, and D. F. Haasi. Fault Tree Handbook. NUREG 0492, Systems and Reliability Research Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission, Washington D.C. 20555, January 1981.

[14] M. L. Visinsky, I. D. Walker, and J. R. Cavallaro. Chapter 8: Robotic Fault Tolerance: Algorithms and Architectures. In M. Jamshidi and P. Eicker, editors, *Robotics and Remote Systems in Hazardous Environments*, pages 53–73. Prentice Hall, Englewood Cliffs, NJ, 1993.

[15] M.L. Visinsky, J.R. Cavallaro, and I.D. Walker. Robotic Fault Detection and Fault Tolerance: a Survey. *Reliability Engineering and System Safety*, 46(4):139–158, 1994.

[16] M.L. Visinsky, J.R. Cavallaro, and I.D. Walker. A Dynamic Fault Tolerance Framework for Remote Robots. *IEEE Transactions on Robotics and Automation*, 11(4):477–491, 1995.

[17] I. D. Walker and J. R. Cavallaro. Failure Mode Analyses of the ORNL MLDUA Manipulator and Hose Management System. Technical Report Internal Study Report, Dept. of Electrical and Computer Engineering, Rice University, Houston, TX, June 1996.

[18] T. Wikman, M. Branicky, and W. Newman. Reflex Control for Robot System Preservation, Reliability, and Autonomy. *International Journal of Computers and Electrical Engineering*, 20(5):391–407, 1994.