Failure Mode Analyses

Robotics Technology Development Program
University R&D Program

Joseph R. Cavallaro and Ian D. Walker

Department of Electrical & Computer Engineering
Rice University, Houston, TX 77251

E-mail: cavallar@rice.edu, ianw@rice.edu

(713) 527-4020

July 1996

Goal of the Project

- Robotic Failure Mode Analyses
- Robot Reliability Analysis
- Fault Tree Development
- Real-Time/Off-Line Analysis
- Fault Detection/Tolerance/Reconfiguration

Our Long Term Project Goals

- Transfer Expertise to DOE Sites
- Utilize Fault Tree Techniques in DOE Robotics Applications
  - Manipulator Level Fault Tree Analysis
  - Robot System Reliability Management
- Rigorous Analysis of Overall System Safety
  - Critical Mix of Discrete and Analog Techniques
  - Develop and Incorporate Fault Detection Methods
  - Sensor Failure Hardware Testbed

Importance/Impact of the Research

- Fault Tree Analysis of Preliminary ORNL Tank Demo System (MLDUA/Hose Management System). Ongoing Analysis.
- Contract with Hanford WHC via Sandia.
  Fault Trees, Specifications and Criteria for LRM Safety
- Interaction with Sandia on Fault Tree Expert System Simulator
- Dissemination of Results - Organized conference session, journal special issues, including upcoming *Reliability Engineering and System Safety* issue on Safety of Robotic Systems.

Schedule and Milestones

- Years One to Four
  - Initial Fault Tree Study
  - Robo-MEDIC Expert System Implementation/Demonstration
  - Fault Trees for Hanford LRM
  - Development of New Fault Detection Methods
  - Programmatic Success Tree Development
- Year Five
  - Quantitative Fault Tree Analysis using ‘Fuzzy’ Data
  - Tree Structure for Cost/Benefit Analysis
  - Initial Fault Tree Analysis of Preliminary ORNL Tank Demo System

Interaction with the DOE Sites and Labs

- ORNL - Development of Fault Trees for Preliminary Design of Tank Demo System (Fall 1995 - ongoing)
- Hanford-WHC - Development of Fault Trees for LRM. Study Report for LRM (April 1994)
- Sandia Labs
  - Porting of Fault Tree Simulator to Integrate with the IGRIP Graphics Package (Fall 1992)
  - Demonstration of Simulator during DOE Forum (Summer 1993)
  - Presentation of LRM Fault Trees during DOE Forum (Summer 1994)

Discussion of Accomplishments

- Software Package Ported to Sandia, Integrated with IGRIP, Demos.
- Study Report and Specification Input for WHC for LRM Project.
- Preliminary Report Detailing Fault Tree Analysis of Tank Demo System for ORNL
- Numerous Journal and Conference Publications Resulting from Work.
- Graduates
  - Monica L. Visinsky, Ph.D. May 1994
  - Deirdre L. Hamilton, Ph.D. May 1996
  - Martin Leuschen, M.S., May 1997 (expected)

Unresolved Needs

- Quantitative Issues: Reliability Prediction
- Effectiveness of Safety Techniques: 'Proofs' of Fault Tolerance?
- Coverage Issues: Fault Detection Verification
- Cost/Benefit Issues for Robot Fault Tolerance

More Details of these Issues to be Presented

New Quantitative Fault Tree Methods

- Failure Probability/Failure Rate Data Inexact for DOE Applications
- Need for Approximate Methods for Reliability Analysis
- Development of Method for Propagating Failure Probability Ranges in Quantitative Fault Tree Calculations
- Can be Viewed as Regular Fault Tree Analysis Using Fuzzy Data

Cost/Benefit Analysis Tree Structure

- Analyze Cost/Benefit Tradeoffs
- Consider Engineering Risk, Economic and Environmental Cost
- Method based on Fault Trees for Engineering Risk - Extra Fields Added for Costs
- Automobile PCV Valve Example

MLDUA Fault Tree Analysis

- MLDUA/Hose Management System (HMS) Planned to be Demonstrated in Tanks at ORNL in 1996
- Initial Fault Tree Study of System Outlined in Volume 2 of this Report
- Study Based on Preliminary Design of MLDUA/HMS System
- Ongoing Study

Current Year Milestones

- Fault Tree Analyses of DOE Robot Systems (Tanks, D&D)
- Development of Quantitative Reliability Techniques for Fault Trees using Fuzzy or Probabilistic Bounds
- Investigation of Provable Fault Tolerance Strategies
- Hardware Testbed for Fault Detection/Tolerance

Summary

- Failure Mode Identification - System-wide Linking via Fault Trees
  - Consistent Means to Analyze Effects from Subsystems of Widely Different Types
  - Qualitative and Quantitative Analysis
  - Inter-relationship with Other Projects: Purdue, CMU, CSM, Florida
- Investigation of Overall Effect of Addition of Fault Tolerance - Coverage Issues
- New Results in Cost/Benefit Analysis
- Transfer of Expertise to Sites: LDUA/MLDUA Example at ORNL Tank Demo Project