Robot Reliability and Fault Trees

Workshop on Fault Tolerant Robots
IEEE International Conference on
Robotics and Automation

Ian D. Walker and Joseph R. Cavallaro

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

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

(713) 527-4020

April 20, 1997

Overview

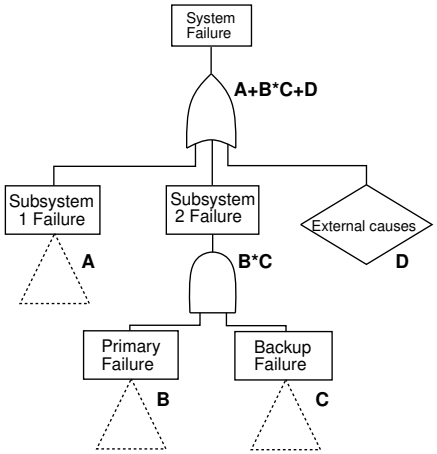
- Robot Reliability Analysis
- Fault Trees
- Approach Sparingly Used in Robotics
- Systemwide Analysis
- Mechanical, Electrical, Electronic and Operator Failure Modes
- Key Actuator and Sensor Failures
- Qualitative Analysis Useful for Reliability Recommendations
- Quantitative Analysis More Complex
- Real-Time/Off-Line Analysis

Fault Trees

- Widely Used Tool in Other Applications
- Logical Interconnection of Failure Events Via Tree Structure
- Straightforward Combination of Failure Events of Different Types
- Useful for Identifying Critical Failure Paths
- Can Include and Manipulate Failure Rates/Probabilities

Symbol	Function
AND gate	All inputs required to produce output event. A fraction, x/y, in the gate means that more than x failures will produce the output event.
OR gate	Any one input event causes the output event.
Rectangle	A malfunction which results from a combination of fault events through logic gates.
Diamond	A fault event for which the causes are left undeveloped.
Circle	A basic fault event. This includes component failures whose frequency and failure mode are known.
Triangle	A suppressed tree. The tree is detailed in another figure.

Fault Tree Analysis Symbols



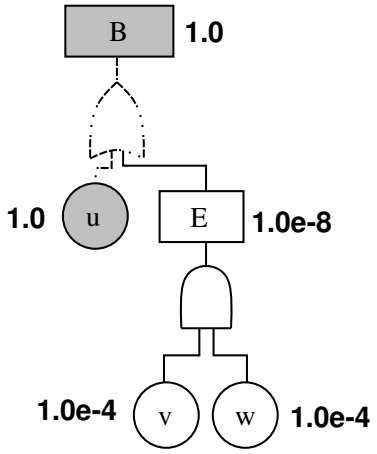
Probability Propagation for Fault Trees.

Example Robot Fault Trees

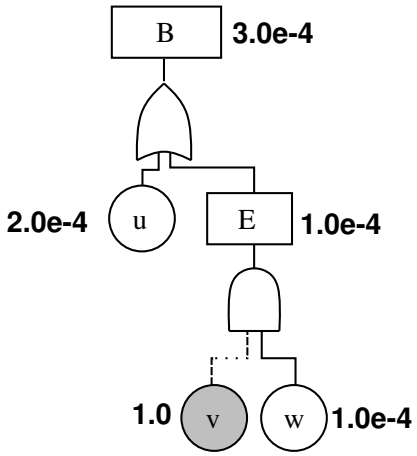
- NASA Flight Telerobotic Servicer
- Oak Ridge - JBF Associates study
- Rice University Eight Joint Manipulators
- Hanford UST Manipulator
- European TELEMAN Nuclear Environment Robots
- Oak Ridge MLDUA Robot System

Failure Modes

- Key: Actuator and Sensor Failures
- Hardware and Software Faults
- Human Reliability Issues



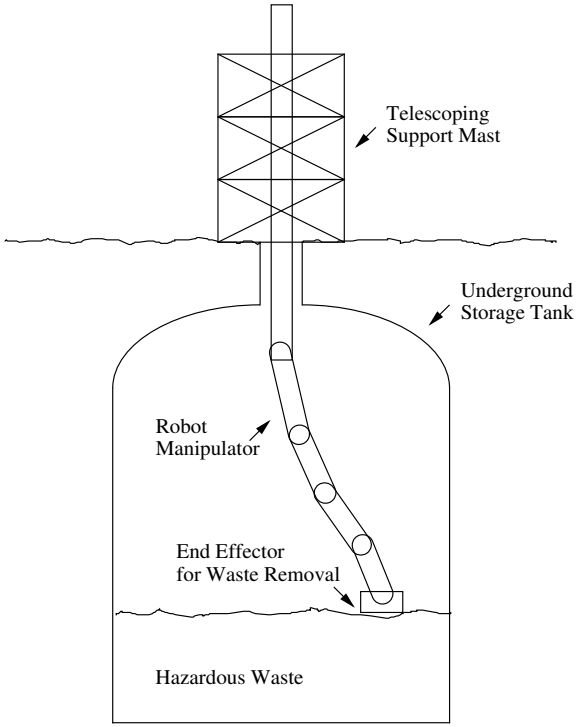
Probability Propagation for Motor Failure.

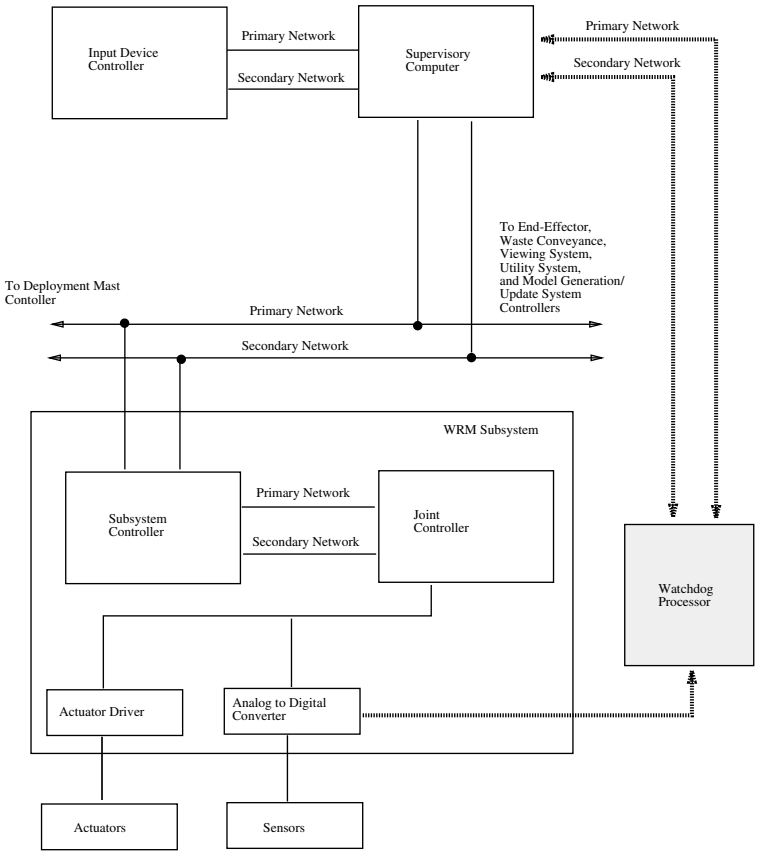


Probability Propagation for Sensor Failure.

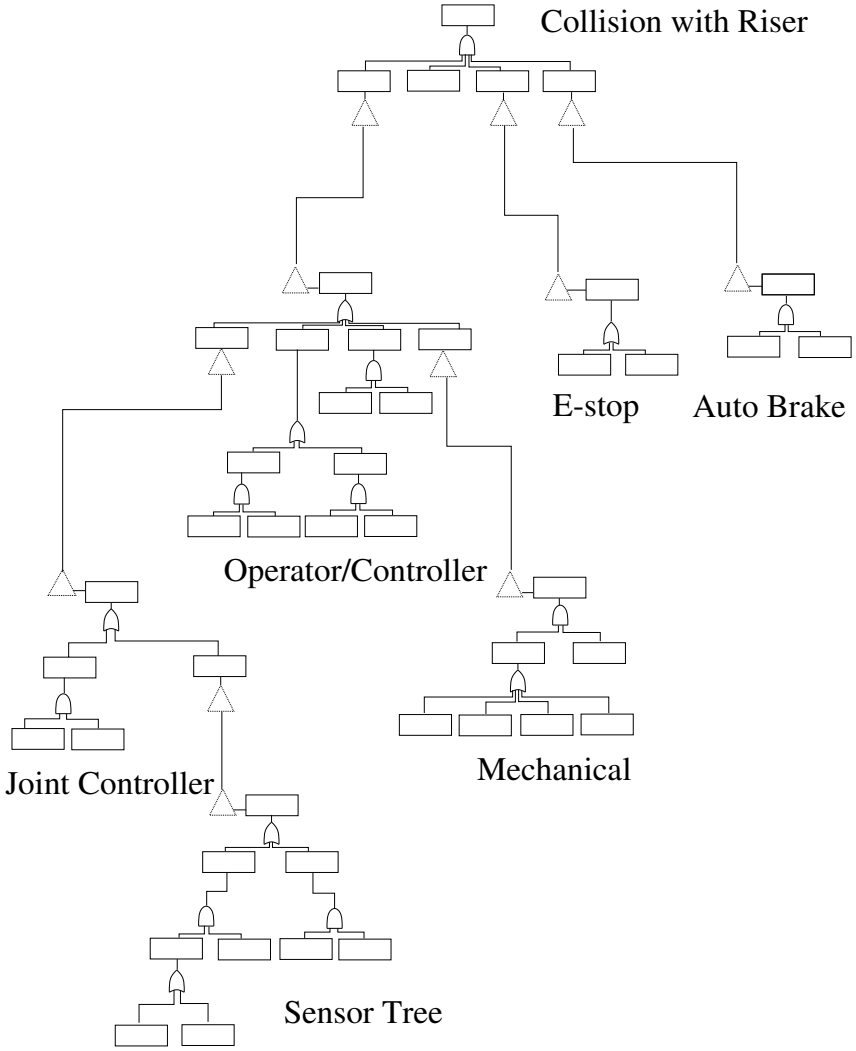
Underground Storage Tank Manipulator Concept Fault Tree Example

On the following pages are a number of example fault trees for an underground storage tank manipulator design. The top is the critical failure event for this scenario and represents the collision of the manipulator with a known vertical obstacle.

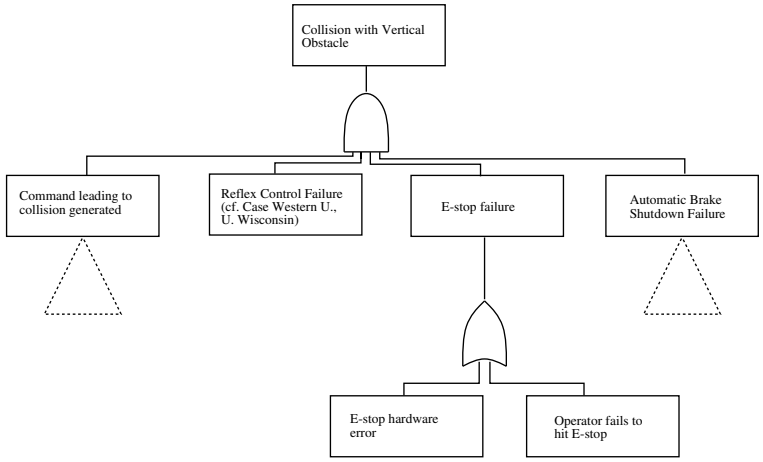




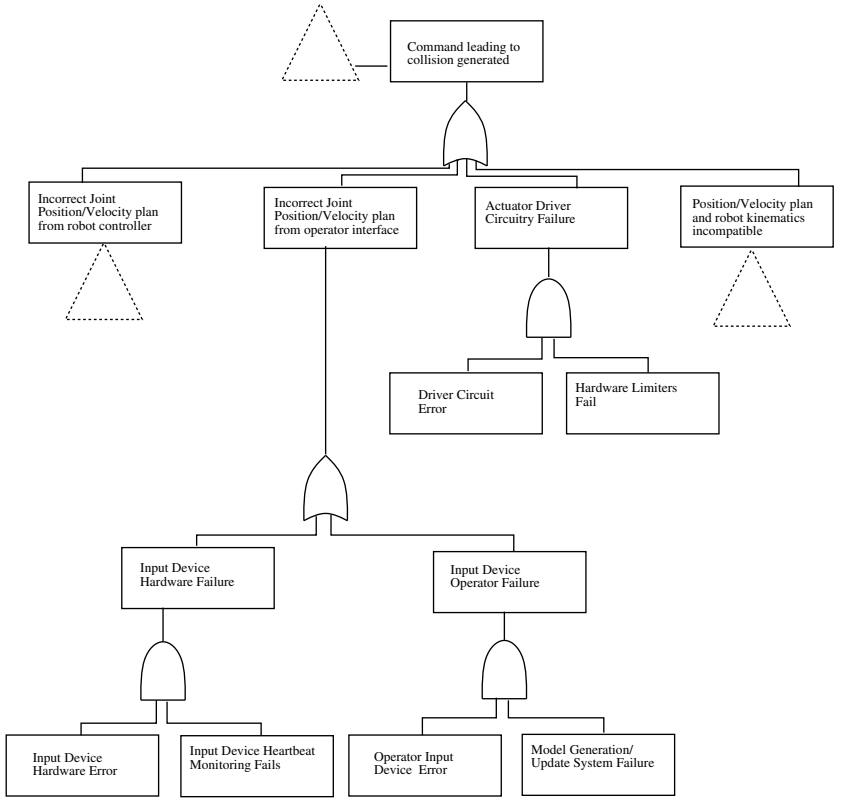
Potential Computer Control Hardware



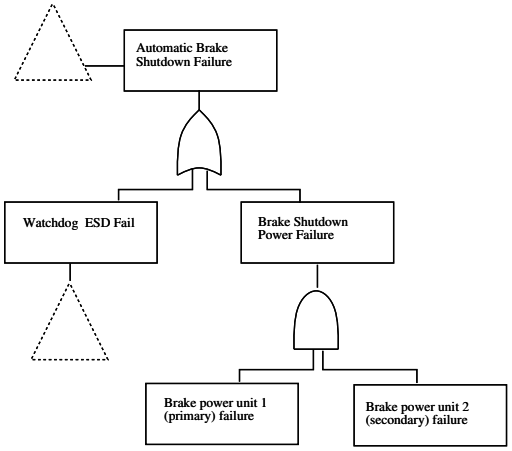
Overall Sketch of Fault Tree.



Top Level Fault Tree - Collision with Vertical Obstacle



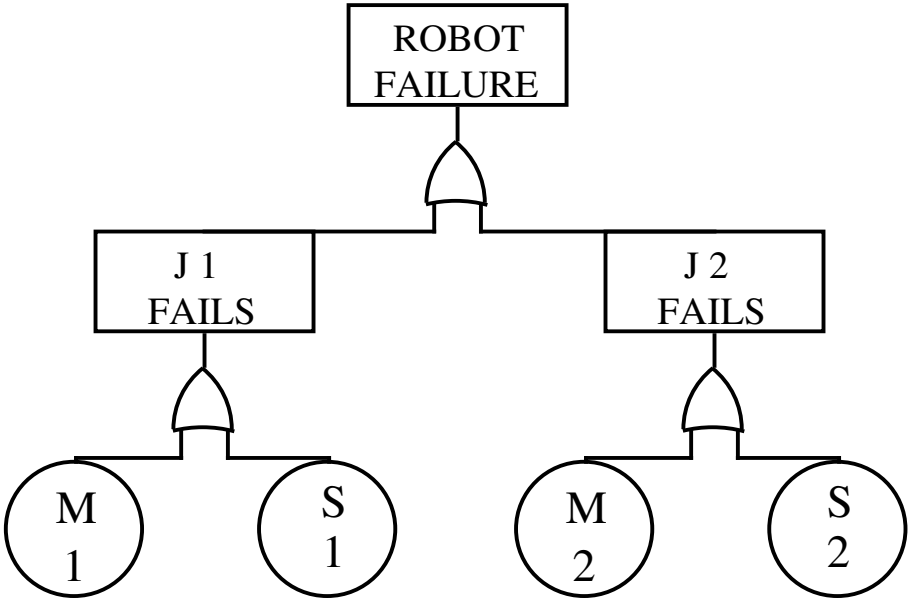
Command Leading to Collision Generated



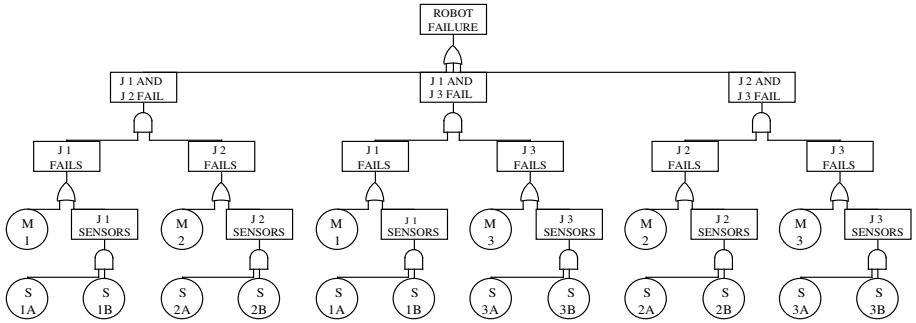
Automatic Brake Shutdown Failure

Quantitative Fault Tree Methods in Robotics

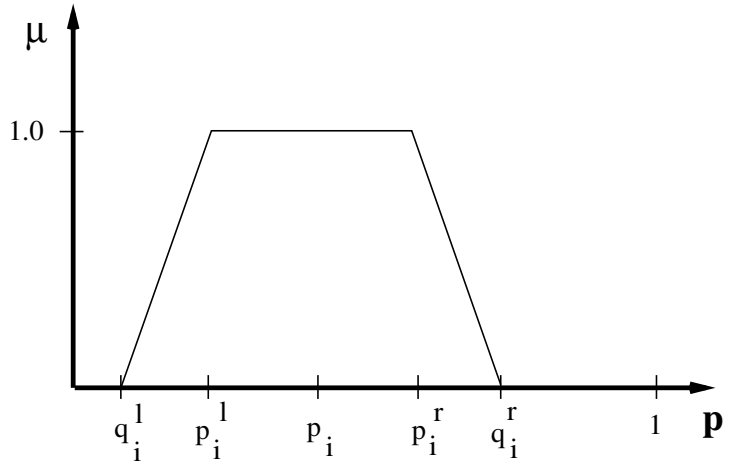
- Open issue
- Failure Probability/Failure Rate Data Inexact for Robotics Applications
- Need for Approximate Methods for Reliability Analysis
- Development of Method for Propagating Failure Probability Ranges in Quantitative Fault Tree Calculations
- Can be Viewed as Regular Fault Tree Analysis Using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



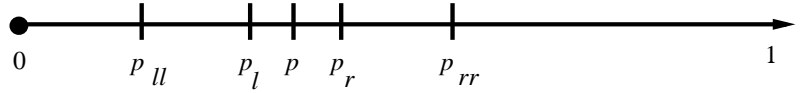
Fault Tree for a Basic Two Joint Planar Robot.



Fault Tree for a Redundant Three Joint Robot with Multiple Sensors.



Interval Probability Data Related to Fuzzy Membership Function.



Failure Probability Interval.

Reliability Estimates for Redundant Planar Robot Components.

Component	p_{ll}	p_l	p_r	p_{rr}
Electric Motor	0.000739	0.00203	0.0416	0.11
Optical Encoder Sensor	0.00124	0.00341	0.0698	0.184

Reliability Estimates for Basic Two Joint Planar Robot Failure.

	p_{ll}	p_l	p_r	p_{rr}
Robot Failure	0.00396	0.0109	0.223	0.588

Exact Value, $p = 0.0490$

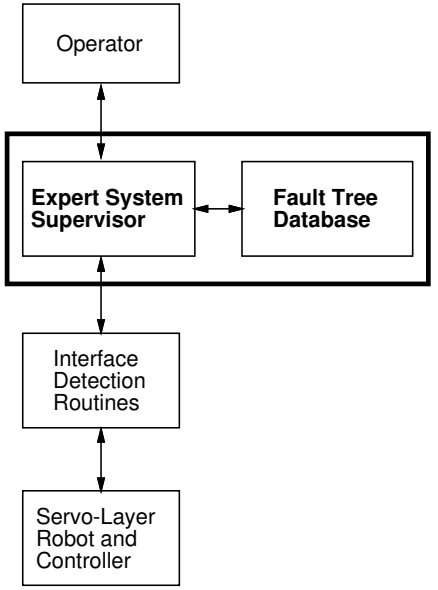
Reliability Estimates for Redundant Planar Robot Failure.

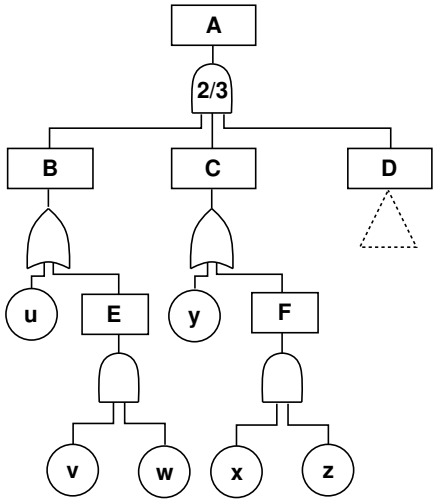
	p_{ll}	p_l	p_r	p_{rr}
Robot Failure	0.00000164	0.0000125	0.00622	0.0534

Exact Value, $p = 0.000268$

Robotic Fault Tolerant Expert System Framework

- Tool for Construction and Modification of Fault Trees
- Allows for Dynamic Failure Modification and Probability Propagation
- Site Independence - Generic and Expandable
- User - Interface



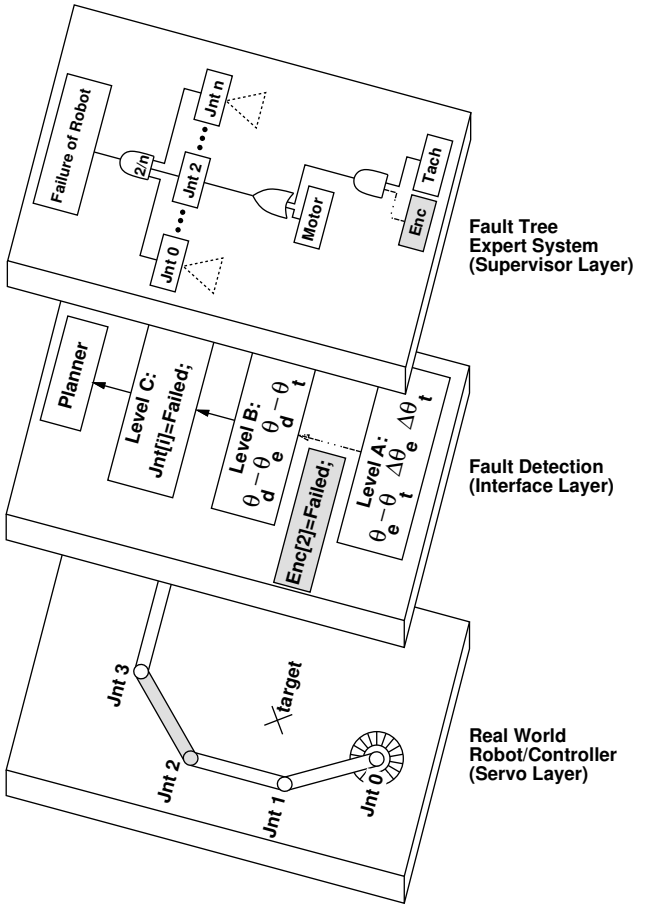


Operator Initializes Expert System with:

```
;structural facts:
(F-AND (out A) (in B C D) (fail-with 2))
(F-OR (out B) (in u E))
(F-AND (out E) (in v w))
(F-OR (out C) (in y F))
(F-AND (out F) (in x z))
....

;initial probabilities:
(prob u 2.0e-4)
(prob v 1.0e-4)
(prob w 1.0e-4)
(prob y 2.0e-4)
(prob x 1.0e-4)
(prob z 1.0e-4)
....
```

Fault Tree Initialization.



Propagation of a Sensor Failure Among Framework Layers.

Further Information

- Fault Tree Handbook, W.E. Vesley et. al., 1981
  US Nuclear Regulatory Commission Wash. D.C.
- *Reliability Engineering and System Safety*
  Special Issue on Safety of Robot Systems
  Volume 53, Number 3, 1996
- *Computers and Electrical Engineering*
  Selected Papers on Robot Fault Tolerance
  Volume 20, 1994
- *Robot Reliability and Safety*
  B.S. Dhillon, Springer-Verlag, NY, 1991
- M.L. Visinsky et. al., 'Robotic Fault Detection and Fault Tolerance: A Survey, *Reliability Engineering and System Safety*, Volume 46, 1994
- Two Sessions on Robot Fault Tolerance, This Conference

Summary

- Robots are Highly Interdisciplinary - Complicates Reliability Analysis
- Fault Trees Thus a Useful Tool for Robotic Applications
- Failure Mode Identification - System-wide Linking via Fault Trees
- Consistent Means to Analyze Effects from Subsystems of Widely Different Types
- Qualitative and Quantitative Analysis Possible
- Off-line and Real-time Analysis Possible
- Some Open Issues in Quantitative Analysis in Robotics