Fault tree based approach for system fault diagnostics

This item was submitted to Loughborough University’s Institutional Repository by the/an author.

Citation: ANDREWS, J.D. and BARTLETT, L.M., 2005. Fault tree based approach for system fault diagnostics. 23rd International System Safety Conference, August 22-26, 2005, San Diego, Westin Hotel

Additional Information:

- This is a conference paper. It was presented at 23rd International System Safety Conference, August 22-26, 2005, San Diego, Westin Hotel.

Metadata Record: [https://dspace.lboro.ac.uk/2134/3646](https://dspace.lboro.ac.uk/2134/3646)

Publisher: © System Safety Society

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
Fault Tree Based Approach for System Fault Diagnostics

L. M. Bartlett and J. D. Andrews:
Aeronautical and Automotive Engineering Department,
Loughborough University, UK

23rd International System Safety Conference 2005
Overview

• Aim of research
• System description
• Diagnostic methods
• Research outcomes
• Conclusions & Summary
Aim of Research

• Background:
  – Several researchers investigated diagnostic methods.
  – Main avenues – sequential tests and real time.
  – Some theoretical, not applied to actual systems.

• Why the need for diagnosis?
  – Improve repair process.
  – Alter missions given system state.
  – Current research lacking in area of real time and multiple faults.
Aim of Research

- Aim:

Develop a diagnostic capability
  - practical
  - real time
  - multiple fault causes
System Description

• Control system
  – V, C, & S.

• Sensors:
  – 1 Flow / No flow pipe 1
  – 2 Flow / No flow pipe 2
  – 3 Level in tank:
    High, Low, Normal
System Description

- Component failures:
  - Pipes blocked (P1B, P2B)
  - Pipes ruptured (P1R, P2R)
  - Tank Ruptured (TR)
  - Tank Leak (TL)
  - Valve fails open (VO)
  - Valve fails closed (VC)
System Description

Assumptions:

Under normal operating conditions:

1. The analysis is performed under steady state conditions.
2. A rupture of the tank means that the outflow from the tank is greater than the inflow.
3. A leak within the tank means the outflow is less than the inflow.
4. Flow in through pipe 1 can be greater than the flow out through pipe 2.
System Description

Modes of Operation:

• Two modes of operation: *normal* and *inactive*.

• **In normal** operation:
  – Flow in section 1.
  – Flow in section 2.
  – Water in the tank normal.

• **In inactive** mode:
  - No flow in section 1.
  - No flow in section 2.
  - No water in the tank.

• Deviations from these expected system symptoms will indicate a fault.
Diagnostic Methods

Use of Fault Trees:

What is a fault tree?:

- Represents failure events.
- Successively breaks down failure event into failure causes.
- Uses deductive logic (What can cause this?).
- Provides information on the combinations of failure causes.

- Two types of fault trees – coherent and non-coherent.
Diagnostic Methods

Coherent & Non-coherent Fault Trees:

- **Coherent**
  - AND / OR logic only
  - Failure events only

![Fault Tree Diagram]

*23rd International System Safety Conference 2005*
Diagnostic Methods

Coherent & Non-coherent Fault Trees:

- **Non-coherent**

  AND / OR logic
  Failure events

  ALSO

  NOT logic
  (functioning events)
Diagnostic Methods

Use of Fault Trees:

The task:
• For any unexpected system observation need to determine cause.

How achieve:
• Fault trees used to represent reasons for sensor readings – i.e. no flow in section 1.
• Sensor reading fault trees can be coherent or non-coherent.
• Cause of unexpected system observation determined by combining appropriate sensor reading fault trees.
Diagnostic Methods

Fault Trees for Sensor Readings:

• Consider the ACTIVE mode:
  – Expected readings:
    • Flow in section 1, flow in section 2, normal level in tank

• Sensor readings of interest:
  – No flow in section 1
  – No flow in section 2
  – High water level in the tank
  – Low water level in the tank
Diagnostic Methods

Example Fault Tree for Sensor Reading:

- **Coherent Fault Tree:**
  - AND/OR logic
  - Failure events only

- **Min Cut Sets:**
  - \{P1B\}
  - \{VC\}
  - \{P2B\}
Diagnostic Methods

Example Fault Tree for Sensor Readings:

Prime Implicant Sets:
- \( \{P_1B.P_1R\} \)
- \( \{VC,VO\} \)
- \( \{P_2B,T_L,P_2R,T_R,VC,VO\} \)

Non-Coherent Fault Tree

Coherent Approx: \( \{P_1B\}, \{VC\}, \{P_2B\} \)
Diagnostic Methods

Combining Fault Tree Information:

• For a given unexpected system observation the relevant sensor reading fault trees can be combined.

• Two methods of combination:
  – Diagnostic Method 1
  – Diagnostic Method 2
Diagnostic Methods

Diagnostic Method 1:

- **System Observation fault tree produced containing:**
  - Observations which *deviate* from the expected normal operation behaviour.
  - The sensor readings which conform to the normal operating states are ignored.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Section 1</th>
<th>Section 2</th>
<th>Tank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal (expected)</td>
<td>Flow</td>
<td>Flow</td>
<td>Normal</td>
</tr>
<tr>
<td>Observed State</td>
<td>Flow</td>
<td>No flow</td>
<td>High</td>
</tr>
</tbody>
</table>
Diagnostic Methods

Diagnostic Method 1:

• **Fault tree for observed system state:**

• **Either coherent or non-coherent fault trees for sensor readings can be used.**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Section 1</th>
<th>Section 2</th>
<th>Tank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Flow</td>
<td>Flow</td>
<td>Normal</td>
</tr>
<tr>
<td>Observed</td>
<td>Flow</td>
<td>No flow</td>
<td>High</td>
</tr>
</tbody>
</table>

23rd International System Safety Conference 2005
Diagnostic Methods

Diagnostic Method 2:

- System Observation fault tree produced containing:
  - Observations which deviate from the expected normal operation behaviour.
  - AND Observations which conform to the normal operating states.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Section 1</th>
<th>Section 2</th>
<th>Tank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal (expected)</td>
<td>Flow</td>
<td>Flow</td>
<td>Normal</td>
</tr>
<tr>
<td>Observed State</td>
<td>No Flow</td>
<td>No flow</td>
<td>High</td>
</tr>
</tbody>
</table>
Diagnostic Methods

Diagnostic Method 2:

- Fault tree for observed system state:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Section 1</th>
<th>Section 2</th>
<th>Tank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Flow</td>
<td>Flow</td>
<td>Normal</td>
</tr>
<tr>
<td>Observed</td>
<td>No Flow</td>
<td>No flow</td>
<td>High</td>
</tr>
</tbody>
</table>

Either coherent or non-coherent fault trees for sensor readings can be used.
Research Procedure

- Each diagnostic method tested using coherent and non-coherent sensor fault trees.
- All possible system observations analysed.
- One example system observation demonstrated.
- Ranking procedure (importance measures) suggested for multiple cause possibilities.
Research Outcomes

Diagnostic Method 1 with coherent sensor fault trees:

- Fault failure causes:
  - P2B.VO
  - TR.VO
  - P1B.VO
  - P1R.VO
  - VC.VO
- Invalid combinations !!
Research Outcomes

Diagnostic Method 2 with coherent sensor fault trees:

- Prime Implicants:
  - \{TR. VO. P1B. VC. P2B\}
  - \{P1R. VO. P1B. VC. P2B\}
- Fault failure causes:
  - \{TR. VO\}
  - \{P1R. VO\}
- Invalid combinations !!

23rd International System Safety Conference 2005
Research Outcomes – Conclusion 1

Coherent Sensor Reading Fault Tree Conclusions:

• Not sophisticated enough to determine a correct fault diagnosis.

• Incorrect fault combinations are produced with both methods 1 and 2.

• Just considering the state of the failed components is not adequate.

• Working components also need to be considered.
Research Outcomes

Diagnostic Method 1 with non-coherent sensor fault trees:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Section 1</th>
<th>Section 2</th>
<th>Tank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Flow</td>
<td>Flow</td>
<td>Normal</td>
</tr>
<tr>
<td>Observed</td>
<td>Flow</td>
<td>No flow</td>
<td>High</td>
</tr>
</tbody>
</table>

- Fault failure cause: P2B.VO
- Correct diagnosis !!

No Flow in section 2

High level in tank

P2B.P2R, TR.TL, P1B.P2B, P1B.TL.TR
P1R.P2B, P1R.TL.TR
VC.VO.P2B, VC.TL.VO.TR
Research Outcomes

Diagnostic Method 2 with non-coherent sensor fault trees:

- Fault failure causes:
  - P2B.VO

- Correct diagnosis !!
Non-coherent Sensor Reading Fault Tree Conclusions:

- Correct failure combinations produced for the example system state observed.

- However invalid combinations produced for other system states.

- Hence, inconsistencies can be found using method 1 where the working states of the system are not considered.
Overall Conclusions

Hence, for **accuracy of diagnosis** the following is needed:

1. Non-coherent fault trees for sensor reading causes.

2. Diagnostic method 2 to construct the observed system state fault tree (i.e. the whole collection of sensor readings, including the expected observations).
Importance Measures

Ranking procedure for multiple fault causes:

• What happens if multiple fault causes are given from the diagnosis?

• Need a method to show most likely cause.

• Fussell-Vesely measure of cut set importance.

• Probabilistic measure defined as:
  • the probability of occurrence of cut set $i$ given that the observed system has failed

\[
\text{Imp} = \frac{\text{probability of cut set occurrence}}{\text{observed system state failure probability}}
\]
Summary

• Two methods have been investigated for diagnosing possible multiple faults within a system.

• Diagnostic method 1 uses information from the deviated observations only.
  – Limitations in producing the correct list of failure combinations using both coherent and non-coherent sensor reading fault trees.
  – Fault combinations have been produced which are invalid when coherent trees have been combined.
  – Combinations produced that could not have occurred due to the status of the normally functioning parts of the system with non-coherent trees.
Summary

• Diagnostic method 2 considered also those parts of the system that are known to be functioning.
  – Inconsistent results produced using coherent sensor reading fault trees for some system observations.
  – Non-coherent fault tree representation of sensor readings proved the most successful as a diagnostic tool.

• The use of importance measures can be used to identify the most likely cause of the system fault when a number of options or possible causes are predicted.
Fault Tree Based Approach for System Fault Diagnostics

Thank you for your attention.

Any questions?????