Fault Tree Based Approach for System Fault Diagnostics

L. M. Bartlett and J.D. Andrews: Aeronautical and Automotive Engineering Department, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK

Keywords: fault diagnosis, fault tree analysis

Abstract

With the ever increasing complexity and functionality of systems the task of identifying and correcting faults is itself a complex issue. Although often designed for reliability, at times components will fail, leading to a decline in system performance or at worse complete system failure. When faults do occur it is imperative they can be diagnosed and ultimately rectified as quickly as possible, minimising the effects of such a failure. In the case of an aircraft system efficient diagnosis can optimise the time to return the aircraft to service. For an unmanned air vehicle diagnosis of the status of the system can mean that missions can be altered or aborted given the faults detected.

Many system failures are not usually the result of one single fault, therefore the ability to diagnose multiple faults is vitally important. A method of finding faults or combinations of faults as they occur is the subject of this paper. The approach uses sensor readings to assess the state of the system. Fault trees, which traditionally provide a diagrammatic description of the causes of system failure, are used to develop causes of a system symptom, as exhibited by the sensor readings. The method diagnoses the faults by considering deviations in the sensor readings from the expected system state.

The primary research has shown the applicability of using a fault tree based approach for system diagnosis. Both coherent fault trees (considering failure events only) and non-coherent fault trees (considering failure and functioning events) have been used to evaluate deviations for an example system. Where combinations of faults result from the diagnosis importance measures can be used to rank the contribution of the failure events and hence highlight the most likely cause of the fault.

Introduction

The concept of fault diagnosis is extremely important with the ever increasing complexity of systems and the demand for enhanced functionality. For system failures or malfunctions methods are required that enable quick detection and diagnosis to allow efficient rectification of the system by repair or alteration of the system functionality to enable some form of mission completion. Fault diagnosis is concerned with identifying and isolating the cause of a system malfunction through conducting some form of test. Testing can occur either continuously, thus detecting faults in real time, or at specific points in time.

Several methods have been devised to enable this system evaluation at specific points in time. The majority of techniques involve a type of testing procedure whereby information about the symptoms of system failure is used (refs. 1-4). Algorithms are implemented to use the minimal number of tests to locate the fault. A FMECA (failure mode, effects and criticality analysis) based method (ref. 5) and a combined FMEA (failure mode and effects analysis) and Fault Tree Analysis method (ref. 6) have also been developed for use in identifying single faults at a point in time. Alternative techniques are to use graphical methods which describe the propagation of faults within a system (ref. 7). The limitation of these procedures is that the output is only a single failure cause. The approaches are not suited to detect multiple failures.

For systems where the failure means a loss of production or a compromise to mission success a real time analysis is required. In addition, with the current reliability demands of systems the configuration is such that more than one component failure is required to cause system failure. Therefore the need to analyse

Originally published by the System Safety Society, in the Proceedings of the 23rd International System Safety Conference, held at San Diego, USA, August 2005

multiple faults is imperative. Some limited work has been performed in this area. The graphical propagation approach has been used to consider multiple failures although the model does not look at the immediate affect on the status of the system (ref. 8). Extension of the testing algorithm approach has been adopted for diagnosis of multiple failures in systems, however, the method takes a considerable length of time to obtain a diagnosis (ref. 9).

A method that can detect these multiple faults is required for application to real industrial problems. Fault trees represent combinations of failure events and can be used to represent the causes of a system state. This paper proposes a method that allows fault diagnosis in real time by considering deviations of the system state from its expected behaviour. Sensors are used to monitor the actual system status and fault trees are used to model the possible sensor deviations. Both coherent fault trees and non-coherent fault trees have been investigated. The coherent tree considers only failure events, whereas the non-coherent fault tree uses success events as well. The application of this method has been carried out by a simple example. When more than one possible fault combination is produced following diagnosis a method has been proposed using importance measures to identify the most likely cause of the failure.

Simple Water Tank System

The system used to illustrate the capability of fault trees as a diagnostic tool is a simple water tank, shown in figure 1.

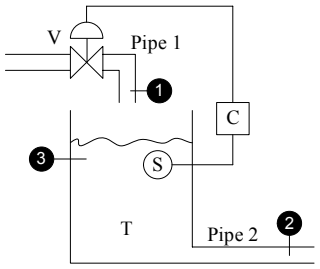

Figure 1 – Simple Water Tank System

The tank has one inlet route for filling the tank and one outlet for the water. Water flows into the tank (T) via pipe 1 and there is a constant flow out of the tank via pipe 2. A control system, in the form of a controller (C), valve (V) and sensor (S), is used to maintain the level of the water in the tank. The flow in through pipe 1 can be greater than the flow out through pipe 2.

To carry out an analysis of the system the following component failure modes are considered, where the failure mode relating to the control valve refers to the whole control system, namely the valve, controller and sensor.

Control Valve fails closed, VC	Control Valve fails open, VO
Pipe 2 Blocked, P2B	Pipe 2 Ruptures, P2R
Pipe 1 Blocked, P1B	Pipe 1 Ruptures, P1R
Tank Leaks, TL	Tank Ruptures, TR

Under normal operating conditions the assumptions of the system are:

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.

To monitor the behaviour of the tank three sensors are placed on the system to; monitor flow / no flow into the tank (referred to as section 1); monitor flow / no flow out of the tank (section 2); and monitor the fluid

level in the tank – normal, high or low. The sensors, shown as black circles in figure 1, are numbered 1 – 3 for the flow in section 1, flow in section 2 and the tank level respectively.

The tank has two modes of operation: normal and inactive. In normal operation the tank will exhibit certain symptoms, namely there will be flow in section 1 allowing water into the tank and there will be flow in section 2 as water will be leaving the tank. Ultimately the level of water in the tank should be normal. When the system is inactive there would be no water entering the tank via section 1, no water exiting via section 2 and no water in the tank. Deviations from these expected system symptoms will indicate a fault. To determine the causes of any faults fault trees can be used.

Coherent Fault Tree Construction for Sensor Deviations

Fault trees can be generated for each possible sensor deviation using either coherent or non-coherent methods. Coherent fault trees are constructed from AND and OR logic and feature only component failure events. The non-coherent method also includes the use of the NOT operator meaning that both component failure and working states are taken into account.

The four possible deviations of the system state for normal operation, with fault trees constructed for each, are:

1) No flow in section 1
2) No flow in section 2
3) High water level in the tank
4) Low water level in the tank

Forming coherent fault trees, involving just component failure events, deviation 1, 'No flow in section 1', is shown in figure 2. No flow is due to either failure within section 1 or activation of the control mechanism to close section 1. Failure within the section is due to failure of pipe 1 or failure of the control valve. Activation of the control system is instigated if a high level in the tank is registered. The cause of this is no flow from the tank, hence pipe 2 is blocked. The failure combinations (minimal cut sets) for no flow in section 1 are therefore: {P1B}, {P2B} and {VC}.

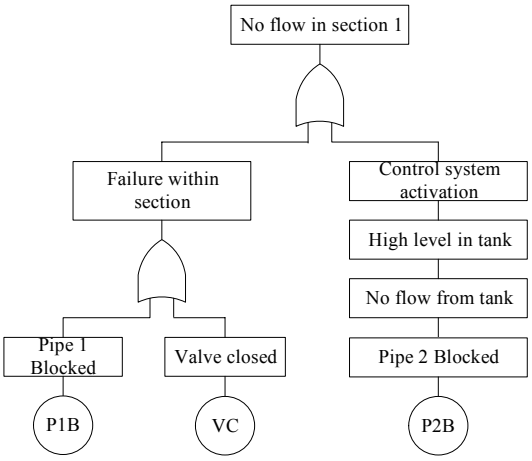

Figure 2 – Fault Tree for 'No flow in section 1'

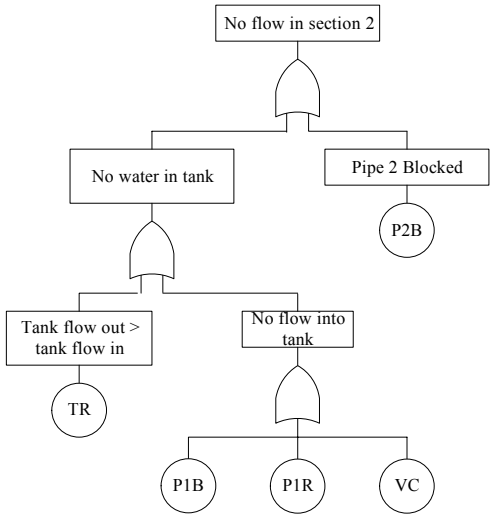

Figure 3 – Fault Tree for 'No flow in section 2'

For the scenario where there is no flow in section 2, shown in figure 3, the immediate causes are due to either pipe 2 being blocked or having no water in the tank. The causes of no water in the tank could be due to either that the flow out of the tank is greater than the flow in or that there is no flow into the tank. A rupture of the tank would mean that the flow out of the tank would be greater than the flow in. For there to

be no flow into the tank pipe 1 could be blocked or ruptured or the valve fails closed preventing water to enter. The minimal cut sets of this scenario are: {P2B}, {TR}, {P1B}, {P1R} and {VC}.

The fault trees representing 'High water level in tank' and 'Low water level in tank' are shown in figures 4 and 5 respectively. The only cause for a high level in the tank is if the valve allowing water in to the tank is fully open, namely VO. For there to be a low level in the tank means that the flow out of the tank must be greater than the flow in. Breaking this down into intermediate causes gives the component failure modes of either a rupture of pipe 2, a rupture of the tank itself or a leak from the tank. The other cause is if there is no flow into the tank. This intermediate event needs to be further examined and results in pipe 1 blocked or ruptured or the valve failed closed. Hence, the minimal cut sets for a low level in the tank are: {P1B}, {P1R}, {VC}, {TL}, {TR}, and {P2R}.

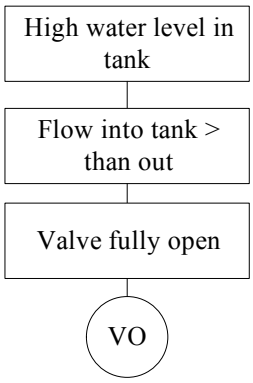

Figure 4 – Fault Tree for 'High level in tank'

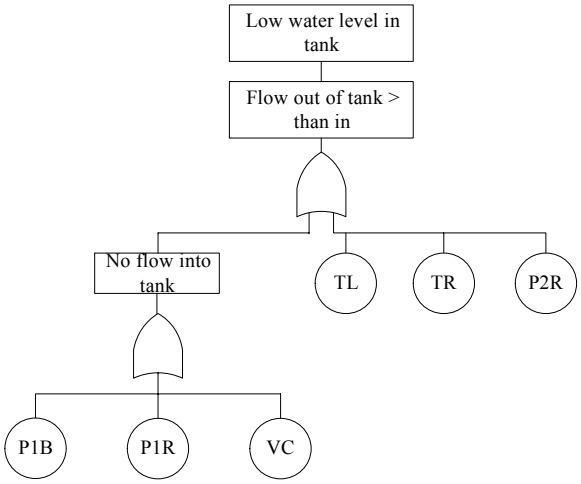

Figure 5 – Fault Tree for 'Low level in tank'

The sensor deviation fault trees can be used to determine the causes of any observed system state. There are two methods which can be adopted for combining these trees, one considering the deviations from normal operation only, the other considering the expected observations as well.

Diagnostic Method 1 – Normal Operation Deviations

The first method investigated to diagnose the causes of a particular system state looks at the *observations which deviate from the expected normal operation behaviour*. The sensor readings which conform to the normal operating states are ignored.

Mode	**Section 1**	**Section 2**	**Tank**
Normal (expected)	Flow	Flow	Normal
Observed State	Flow	*No flow*	*High*

Table 1 – Observed and Expected System States

To illustrate the diagnostic method consider the observed system state shown in row 3 of table 1. There are two deviations from the expected normal operation state – in section 2 and in the tank. To use method 1 to diagnose the faults within the system these deviated observations are combined to yield the top event structure shown in figure 6.

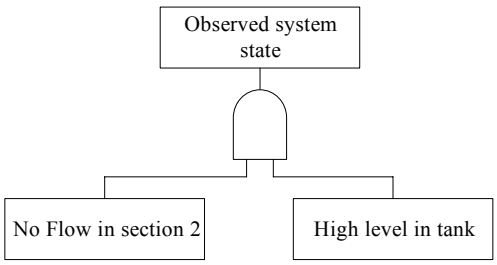

Figure 6 –Top Event Structure for Observed System State Using Diagnostic Method 1

Using standard fault tree qualitative techniques the possible causes of the observed system state are: {P2B.VO}, {TR.VO}, {P1B.VO}, {VC.VO}, and {P1R.VO}. With closer inspection of these fault combinations, although the minimal cut sets of the individual fault trees are correct, it is evident that some of the combinations for this scenario will not actually cause the top event. For example, consider the combination {TR.VO}. If the tank was ruptured (TR) this would mean that there would be no flow in section 2 as there would be no water to flow along this pipe. With the valve failing open (VO) this would mean a constant flow of water into the tank but the water would be leaving the tank through the rupture point and therefore the water level would not be high. The validity and associated reasonings of the other combinations are explained in table 2. The only cause of the observed scenario can be {P2B.VO}, pipe 2 blocked and control valve failed open. To check the acceptability of this possible fault cause evaluation against the expected sensor readings can be made. It is also known that there is flow in section 1, the {P2B.VO} combination would be consistent with this outcome.

	No flow in section 2	**Water level high**	**Comments**
P2B.VO	Yes	Yes	Agrees with top event
TR.VO	Yes	No	Low / no water as tank rupture
P1B.VO	Yes	No	Level not high as entry blocked via pipe 1
VC.VO	IMPOSSIBLE!		Component can not fail in two states
P1R.VO	Yes	No	Level not high as inlet route failed

Table 2 – Checks of Scenario Minimal Cut Sets

Diagnostic Method 2 – Observed Deviations and Expected States

With the coherent fault trees just using information relating to the failed components does not provide sufficient information to correctly diagnose the faults present. Given that it is also known that some components are functioning in the system, namely those related to the expected system observations, these can be used to provide extra information. The second diagnostic method investigated looks at the causes of the *observable system states both for the deviations from normal operation and those expected states*. Including the expected states will eliminate failures which would cause the problem indicated but if they occurred would also cause the problem on the sections where normal observations were seen. Using the observed system state from table 1, the top event of the fault tree contains the two deviated observations 'No flow in section 2' and 'High fluid level in tank', and also the expected state NOT 'No flow in section 1' (as shown in figure 7).

The causes of no flow in section 2 are {P2B}, {TR}, {P1B}, {VC} and {P1R}. The cause of a high level in the tank is {VO}, and the cause of NOT no flow in section 1 is $\{\overline{P1B}.\overline{VC}.\overline{P2B}\}$ where the '– ' refers to the working state of the component. Using AND logic to relate the three inputs gives combinations of working and failed components referred to as prime implicant sets, these are:

1. $TR.\overline{P1B}.\overline{VC}.\overline{P2B}.VO$
2. $P1R.\overline{P1B}.\overline{VC}.\overline{P2B}.VO$

As the main concern is the failure events leading to a certain system behaviour a coherent approximation can be taken from the implicant sets. This assumes that the working states are almost certain to happen. Therefore, the coherent approximation of each implicant set is: {TR.VO} and {P1R.VO}. From table 2 it is evident that both of these combinations will not produce a high level in the tank and therefore will not lead to the occurrence of the top event. Ultimately these causes are incorrect.

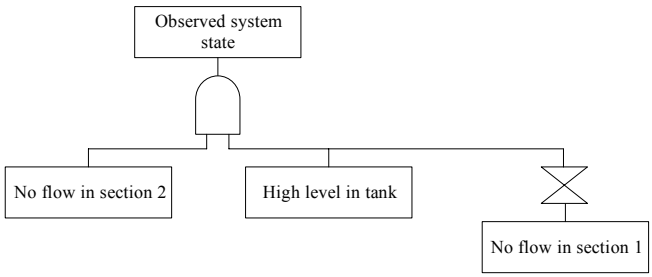

Figure 7 –Top Event Structure for Observed System State Using Diagnostic Method 2

Coherent Sensor Deviation Fault Tree Conclusions: Even for this simple tank system these approaches using coherent fault tree structures (those considering only component failures) for the sensor readings is not sophisticated enough to determine a correct fault diagnosis. It has been illustrated that incorrect fault combinations are produced with both methods. Just considering the state of the failed components is not adequate. The state of the working components within the system also need to be considered, hence, non-coherent fault trees are required.

Non-coherent Sensor Deviation Fault Tree Construction

Non-coherent (N-C) fault trees consider both failure and success events. Fault trees incorporating these states can be established for each of the four possible sensor deviations as shown in figures 8 - 11. Considering the 'No flow in section 1' fault tree, like in the coherent case, the initial causes of no flow are a failure within section 1 or an activation of the control system. Failure within section 1 can be broken down into failure of the pipe or failure of the valve. Failure of the pipe is due to the failure mode pipe 1 blocked (P1B), but also as the working states are considered, this is combined using AND logic with the pipe NOT ruptured ($\overline{P1R}$). This is true for the valve failure also, where the combination of failed and working states refer to the valve failing closed and it NOT failing open respectively. For the right hand branch of the fault tree, a 'High level in the tank', the causes are due to pipe 2 being blocked AND the tank functionality being maintained AND the control system working. The logic for the trees in figures 9 – 11 is broken down in a similar manner.

The causes (prime implicant sets) for each individual fault tree are summarised in table 3. These fault trees can be combined using methods 1 and 2 to yield causes of any system deviation.

No flow in section 1	$\{P1B.\overline{P1R}\}, \{VC.\overline{VO}\}, \{P2B.\overline{TL}.\overline{P2R}.\overline{TR}.\overline{VC}.\overline{VO}\}$
No flow in section 2	$\{P2B.\overline{P2R}\}, \{TR.\overline{TL}\}, \{VC.\overline{VO}.\overline{P2B}\}, \{VC.TL.\overline{VO}.\overline{TR}\}, \{P1B.\overline{P2B}\}, \{P1B.TL.\overline{TR}\}, \{P1R.\overline{P2B}\}, \{P1R.TL.\overline{TR}\}$
High level in tank	$\{VO.\overline{TL}.P1R.\overline{TR}.\overline{VC}.P1B.\overline{P2R}\}$
Low level in tank	$\{VC.\overline{VO}.\overline{P2B}.\overline{P2R}.\overline{TL}.\overline{TR}\}, \{TR.\overline{TL}\}, \{P1R.\overline{P2B}.\overline{P2R}.\overline{TR}.\overline{TL}\}, \{P1B.\overline{P2B}.\overline{P2R}.\overline{TR}.\overline{TL}\}, \{\overline{P1B}.TL.\overline{TR}.\overline{P2B}.\overline{VC}.\overline{VO}.\overline{P1R}\}, \{\overline{P1B}.\overline{P2B}.\overline{VC}.\overline{VO}.\overline{P1R}.P2R\}$

Table 3 – Prime Implicant Sets for the Four Symptoms

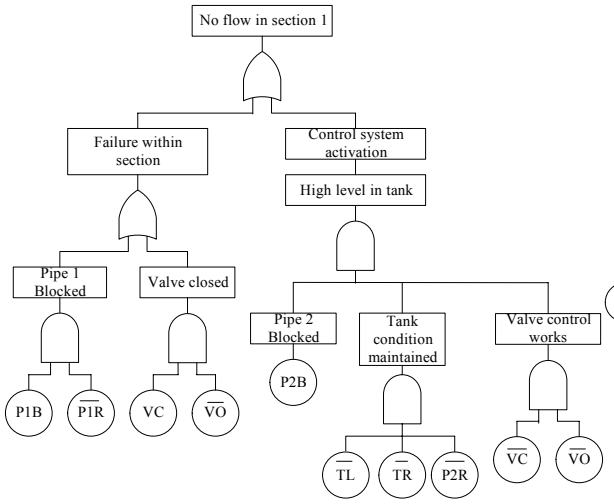

Figure 8 – N-C Fault Tree for 'No flow in section 1'

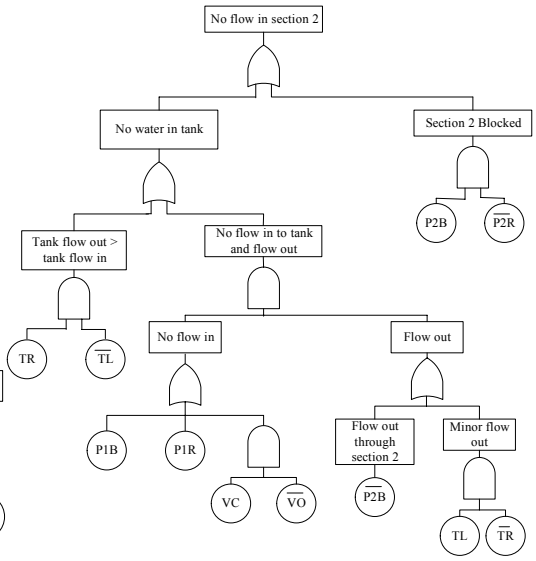

Figure 9 – N-C Fault Tree for 'No flow in section 2'

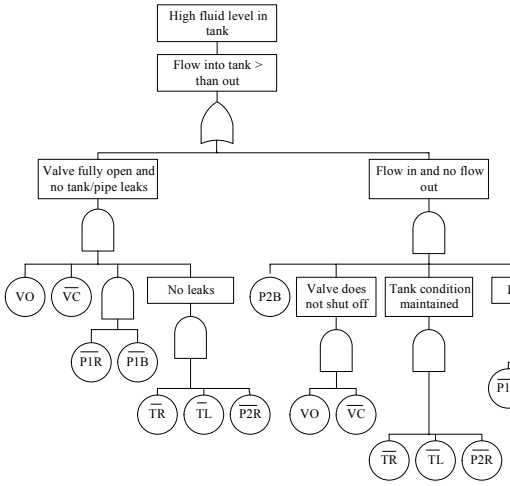

Figure 10 – N-C Fault Tree for 'High fluid level in tank'

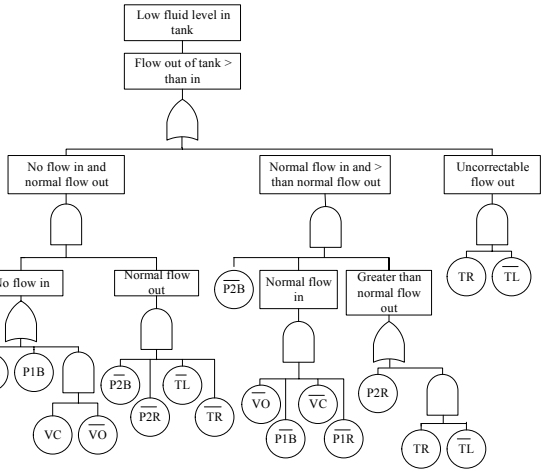

Figure 11 – N-C Fault Tree for 'Low fluid level in tank'

Diagnosis Using Non-Coherent Sensor Deviation Fault Trees

Diagnostic Method 1 – Normal Operation Deviations: The top event structure for the observed system state is created considering the deviated sensors only, as shown in figure 6, but using the non-coherent fault trees. This means the prime implicants from column 2 of table 3 are 'ANDed' with those in column 3. Using this logic means that several combinations are impossible due to the occurrence of a failed and working state of the same component. For example, using the '.' symbol to represent an AND gate, $(\mathrm{TR}.\overline{\mathrm{TL}}).(\mathrm{VO}.\overline{\mathrm{TL}}.\overline{\mathrm{P1R}}.\overline{\mathrm{TR}}.\overline{\mathrm{VC}}.\overline{\mathrm{P1B}}.\overline{\mathrm{P2R}})$ has the combination $TR.\overline{TR}$ which is not possible, and therefore this combination is automatically removed in the analysis. The end result gives the cause of the observed scenario as:

$$\mathrm{P2B}.\overline{\mathrm{P2R}}.\mathrm{VO}.\overline{\mathrm{VC}}.\overline{\mathrm{P1R}}.\overline{\mathrm{P1B}}.\overline{\mathrm{TR}}.\overline{\mathrm{TL}}$$

The coherent approximation is {P2B.VO} which is the correct cause.

Diagnostic Method 2 – Observed deviations and Expected States: Creating the same top event structure as in figure 7 requires the prime implicants for NOT no flow in section 1 to be combined with the result from method 1. The causes of NOT no flow in section 1 using the non-coherent sensor deviation fault tree are:

$\{\overline{P1B}.VC.\overline{P2B}\}, \{\overline{P1B}.\overline{VC}.TL\}, \{\overline{P1B}.\overline{VC}.P2R\}, \{\overline{P1B}.\overline{VC}.TR\},$
$\{\overline{P1B}.\overline{VC}.VO\}, \{\overline{P1B}.VO\}, \{P1R.\overline{VC}.\overline{P2B}\}, \{P1R.\overline{VC}.TL\},$
$(P1R.\overline{VC}.P2R\}, \{P1R.\overline{VC}.TR\}, \{P1R.\overline{VC}.VO\}, \{P1R.VO\}$

Hence, the necessary and sufficient cause of the observed system state is:

$$\overline{P1B}.VO.P2B.\overline{P1R}.\overline{VC}.\overline{P1R}.\overline{TR}.\overline{TL}$$

Therefore the method has identified the correct failure cause of {VO.P2B}.

In this example the solutions using diagnostic methods 1 and 2 with the non-coherent trees is the same, indicating that either approach could be adopted. However, with further investigation it can be shown that the first method does not always yield the correct fault causes. Consider the observed system state shown in table 4, where the deviated observations are the flow in section 2 and the level in the tank.

Mode	**Section 1**	**Section 2**	**Tank**
Normal (expected)	Flow	Flow	Normal
Observed State 2	Flow	*No flow*	*Low*

Table 4 – Observed System State 2

Using diagnostic method 1 the deviations of 'No flow in section 2' and 'Low level in the tank' are combined. Taking the coherent approximation of the prime implicants produced gives four possible fault causes, {TR}, {VC}, {P1B} and {P1R}. Examining these indicates that although {VC} and {P1B} would cause the top event, they are not consistent with the fact that there is flow in section 1. Therefore these two possibilities are incorrect. Using diagnostic method 2, whereby NOT 'No flow in section 1' is added as an input to the top event along with those from method 1, the resulting failure combinations are {P1R} and {TR} as desired.

Non-coherent Sensor Deviation Fault Tree Conclusions: Using diagnostic methods 1 and 2 with non-coherent fault trees for the sensor deviations has yielded the correct failure combinations for the initial scenario investigated. However further examination of the methods considering the other possible system states has concluded that inconsistencies can be found using method 1 where the working states of the system are not considered. 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 fault tree for system symptoms (i.e. the whole collection of sensor readings, including the expected observations).

Use of Importance Measures

As the complexity of the system increases the greater the likelihood that more than one fault combination results following diagnosis. In the situation that there are several possibilities for the cause of a system scenario a mechanism is required to direct attention toward the real cause as quickly as possible. This paper proposes that importance measures for the failure combinations can be used. Therefore the failure combination which has the largest contribution to system failure can be investigated as the potential cause first. If through testing or inspection components within the proposed failure combination are working then the next ranked combination can be examined, until the actual fault combination is found.

The advised importance measure is the Fussell-Vesely measure of cut set importance (ref. 10). This is a probabilistic measure defined as the *probability of occurrence of cut set i given that the system has failed* (equation 1).

$$I_{C_i} = \frac{P(C_i)}{Q_{SYS}(\mathbf{q}(t))} \qquad \text{(eqn.1)}$$

where $P(C_i)$ is the probability of cut set i occurrence, and $Q_{SYS}(\mathbf{q}(t))$ is the probability of system failure.

To illustrate how this can be applied, consider the second observed system state (given in table 4). The fault causes are {P1R} or {TR}. The importance ranking for each component can be calculated as follows:

The logic expression representing system failure: SYS failure = P1R + TR.
The probability expression is: P(SYS failure) = P(P1R) + P(TR) – P(P1R.TR)

If the failure probabilities are 0.0003 and 0.0004 for P1R and TR respectively, the probability of the top event is 6.998×10^{-4}. Hence the importance rankings for cut set 1 (P1R) and cut set 2 (TR) are:

$$I_{C_1} = \frac{0.0003}{6.998x10^{-4}} = 0.429 \qquad I_{C_2} = \frac{0.0004}{6.998x10^{-4}} = 0.572$$

Therefore the importance ranking gives cut set 2, {TR}, as the greatest contributor to the observed system state. This combination would be investigated first as the cause of the system deviation. For cut sets that contain more than one component the probability of each component is multiplied together to produce the cut set failure probability.

Conclusions

Two methods have been investigated as to their potential for diagnosing faults in a system given observed deviations in the system behaviour from that expected. The first method uses information from the deviated behaviour only. The method has shown limitations in producing the correct list of failure combinations for the fault using both coherent and non-coherent sensor deviation fault trees. Fault combinations have been produced which are invalid when coherent trees have been combined and produced combinations that could not have occurred due to the status of the normally functioning parts of the system with non-coherent trees. The second method investigated aimed to overcome these inadequacies by considering also those parts of the system that are known to be functioning. When using non-coherent sensor deviated fault trees this eliminated the previous problems for the given example system. Ultimately, method 2 using deviated and expected sensor readings in conjunction with a non-coherent fault tree representation of the cause of sensor deviations themselves has 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.

References

1. Zuzek A., Biasizzo A. and Novak F., “Towards a General Test Presentation in the Test Sequencing Problem”, Proceedings of the 2nd International On-Line Testing Workshop, IEEE Computer Society Press, Biarritz, France, 236-237, 1996.
2. Zuzek A., Novak F., Biasizzo A., Savnik I. And Cestnik B., “Sequential Diagnosis Tool for System Maintenance and Repair”, Electrotechnical Review, **62**:224-231, 1995.
3. Biasizzo A., Zuzek A. and Novak F., “Sequential Diagnosis With Asymmetrical Tests”, The Computer Journal, **41** [3] 163-170, 1998.

4. Pattipati K. R. and Alexandridis M. G., "Application of Heuristic Search and Information Theory to Sequential Fault Diagnosis", IEEE Transactions on Systems, Man and Cybernetics, **20** [4] 872-887, 1990.
5. Price C., "Computer-Based Diagnostic Systems", Springer-Verlag London Limited, 1999.
6. Paasch R. and G. Mocko, "Incorporating Uncertainty In Diagnostic Analysis Of Mechanical Systems", Proceedings of the 2002 ASME Design Theory and Methodology Conference, Montreal, QB, October 2002.
7. Rao N. S. V., "Expected-Value Analysis of Two Single Fault Diagnosis Algorithms", IEEE Transactions on Computers, **42** [3] 272-280, 1993.
8. Pattipati K.R., "Computationally Efficient Algorithms for Multiple Fault Diagnosis in Large Graph-Based Systems", IEEE Transactions on SMC: Part A – Systems and Humans, **33** [1] 73-85, 2003.
9. Shakeri M., Raghavan V., Pattipati K. R. and Patterson-Hine A., "Sequential Testing Algorithms for Multiple Fault diagnosis", IEEE Transactions on Systems Man and Cybernetcis - Part A: Systems and Humans, **30** [1] 1-14, 2000.
10. J.D.Andrews and T.R.Moss. "Risk and Reliability Assessment", 2nd edition, PEP, 2002.

Biography

Lisa M Bartlett; Aeronautical and Automotive Engineering Department; Loughborough University; Loughborough; LE11 3TU; U.K, telephone – +44 (0)1509 227 276, facsimile – +44 (0)1509 227 275, e-mail: L.M.Bartlett@lboro.ac.uk.

Dr. Lisa Bartlett is a lecturer in the Department of Aeronautical and Automotive Engineering at Loughborough University. She is one of three academic members of staff within the Reliability Research Group of the department. She gained her PhD in Fault Tree Analysis methods in 2000 from Loughborough University. Her PhD research focused on the Binary Decision Diagram approach, an alternative analysis method for fault tree analysis. Her current research interests are in safety system optimisation, binary decision diagrams and fault diagnostics.

John D. Andrews, Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK, telephone – +44 (0)1509 227 286, facsimile – +44 (0)1509 227 275, e-mail – J.D.Andrews@lboro.ac.uk

John Andrews is Professor of Systems Reliability in the Department of Aeronautical and Automotive Engineering. He joined Loughborough University in 1989 having previously gained nine years industrial research experience with British Gas. His current research interests concern the assessment of the safety and risk of potentially hazardous industrial activities. This research has been heavily supported by industrial funding. Over recent years grants have been secured from BAE Systems, MOD, Rolls-Royce, ExxonMobil and Bechtel. Professor Andrews has over one hundred journal/conference publications along with a jointly authored book 'Reliability and Risk Assessment' which is now in its second edition.