Comparison of Digraph and Fault Tree Based Approaches for System Fault Diagnostics

L.M. Bartlett, E.E. Hurdle & E.M. Kelly
Aeronautical and Automotive Engineering Department, Loughborough University, Loughborough, UK.

ABSTRACT: The issue of fault diagnosis has become ever prevalent in engineering systems. Information concerning possible failures within a system can help to minimise the disruption to the functionality of the system by allowing quick rectification. Traditional approaches to fault diagnosis within engineering systems have focused on sequential testing procedures and real time mechanisms. Both methods have been predominantly limited to single fault causes. Latest approaches also consider the issue of multiple faults in reflection to the characteristics of modern day systems designed for high reliability. The bases of these approaches are the fault tree analysis technique and the method of digraphs. Both use a comparative approach to consider differences between actual system behaviour and that expected. This paper focuses on reviewing the developments with these methods to diagnose faults within an aircraft fuel system and to compare their effectiveness and future potential.

1 INTRODUCTION

Failures within a system can cause disruptions to operational functionality. The ability to diagnose a fault when it occurs is the first step to minimising this failure disruption time. Several techniques have focused on identifying faults at a specific point in time using a series of testing procedures [Novak et al. 2000, Pattipati & Alexandridis, 1990]. The methods work using information regarding symptoms exhibited by the system when a fault is present. Tests are carried out on the system to 'hone in' on the fault cause(s). These approaches have been found to be effective in identifying single faults although have more difficulty coping with the complexities of multiple fault combinations (especially with dependency issues). In addition, these methods are suitable for systems which have a period of inactivity where testing can occur at appropriate times without disruption. This allows identification of any faults prior to operation. However, this type of procedure is not effective if failure occurs between the specified points of diagnosis as the maximum recovery time of the system is not utilised without immediate detection. Thus, the characteristics associated with modern day systems require real time diagnosis and to incorporate both adaptability and identification of multiple faults (Venkatasubramanian et al. 2003). Systems usually operate in more than one mode, for example, an aircraft fuel system can be used in flight and during refuel, and so an ideal situation involves being able to adapt the scope of the diagnostics procedure.

In trying to deal with diagnosis of multiple faults extensions to the testing procedures have been developed (Shakeri et al. 2000), in addition such tools as genetic algorithms (Yangping, 2000) have been implemented, both with limited success. Other recent approaches have used reliability assessment tools such as failure modes and effects analysis (Price 1997, Price & Taylor 1997), fault tree analysis (Hurdle et al. 2005) and a combination of both (Henning & Paasch 2000). Variability in performance of these methods is exhibited with increased system complexity. The method of digraphs has been used for limited multiple failures (Iverson & Patterssine-Hine 1995) identifying the potential for real-time automated monitoring and diagnosis, with improvement needed in the number of faults revealed.

With a limitation on the number of effective real time multiple fault diagnostic tools currently in the literature, this paper compares the most recent fault tree analysis and digraph based methods. The review focuses on the application to an aircraft fuel rig system. Section 2 reviews the application fuel system in detail. Section 3 explains each of the individual diagnostic methods. Section 4 considers the

results obtained from the diagnostic methods when applied to the fuel rig. A discussion is provided in Section 5 and Section 6 gives conclusions to the research.

2 FUEL SYSTEM

2.1 *System Architecture*

The purpose of a fuel system is to reliably provide an adequate amount of clean fuel at the right pressure to the engines during all phases of flight. A schematic of the experimental fuel rig utilised in this research is presented in Figure 1. It is representative of a modern aircraft fuel system, the only difference being that water is used as the fluid representative of the fuel.

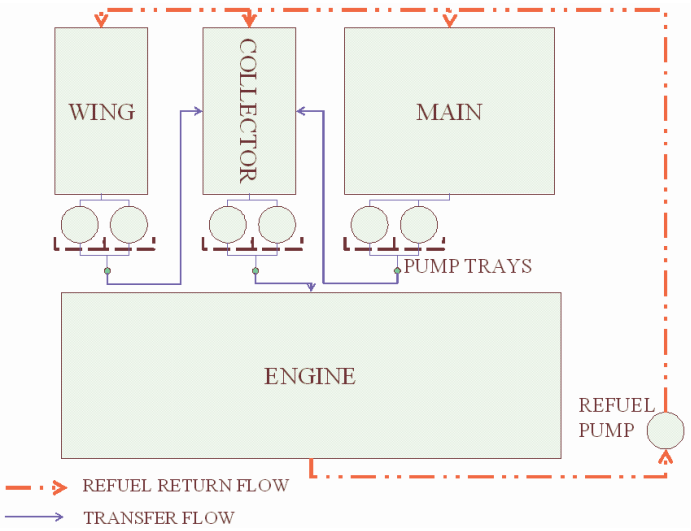

Figure 1. Fuel Rig Schematic

Three tanks (Main, Wing and Collector) form the fuel system which feeds the engine. Each tank has two associated pump trays encompassing a peristaltic pump, a pressure relief valve, powered and manual isolation valves and a pressure regulating valve.

The collector tank provides the only feed of fuel to the engine tank which occurs via a parallel set up of two pumps. The main storage of fuel for the collector tank is via the main tank. Two pumps, connected in parallel, pump fuel from the main tank to the collector tank. The auxiliary storage tanks of the aircraft fuel system are represented by the wing tank. Like the main tank, two parallel pumps transfer fuel from the wing tank to the collector tank. A large single tank at the base of the fuel rig represents an aircraft engine. A final pump, the centrifugal refuel pump, transfers fuel back into the active supply tanks from the engine tank (representative of refueling). Complete drainage of the fuel system is conducted through utilising the engine tank drain valve. Each of the three active supply tanks are also connected to the engine tank via a manually operated dump valve (to represent the dump situation of a real aircraft system).

The two main modes of operation are ‘active’ and ‘dormant’. In the active mode fluid is transferred from the collector tank to the ‘engine’ (engine tank). As the collector tank level decreases the transfer of fuel from the wing and main tanks to the collector tank commences. The tank pumps are switched on and powered isolation valves opened. In the dormant mode the system is in standby, no transfer of fuel occurs between the active supply tanks and the engine. The tank pumps are switched off and powered isolation valves shut.

Two further modes which can be considered are ‘refuel’ and ‘fuel dumping’. Refuelling involves transferring fluid from the engine tank store to the three active supply tanks. During fuel dumping the system is drained of all fluid.

2.2 *Component Failure Modes*

There are 43 different component failure modes considered in the analysis, which may affect the functionality of the fuel rig system. Each component failure mode is allocated a code which contains the relevant component identification number. The majority of the failure modes (30) are associated with one of six valve categories. The valve genres comprise pressure relief (PSV), powered isolation (IVP), pressure regulating (BP), block bleed (BBV), and drain (IV). All of the valve classes can fail blocked or leaking. Partial blockage failures could also affect all valves apart from those in the block bleed category. In addition, pressure relief, powered isolation, block bleed and drain valves can fail either open or closed. A final failure, only connected to pressure relief and powered isolation valves, involves failing stuck in an intermediate position.

The peristaltic pumps, located in each tank feed line, have four related failure modes whilst the centrifugal pumps, utilised in both the transfer and refuel, have three. The pumps can fail on, shut off or leaking. A further failure mode only associated with the peristaltic pumps involves a mechanical failure. Each tank has two failure modes; tank ruptured or leaking. There are four possible pipe component failures. These relate to ruptures, leakages, and complete or partial blockages of individual pipes.

2.3 *Monitoring System Operational Behaviour*

The fuel system status can be obtained using the information from three types of sensors associated within the tanks. These are level, flow and pressure transmitters. Distributed throughout the system are four level transmitters (one in each of the main, wing, collector and engine tanks), seven flow transmitters (two for each of the wing, main and collector

tanks, one for the engine tank), and six pressure transmitters (two for each of the main, wing and collector tanks). For diagnostics the level transmitters allow categorization of the fuel level into high (above required level), low (below pump shut off level), required level (maximum refuelling level), fine section (between pump shut off and required refuelling level), pump shut off (level at which insufficient fuel for transfer) or empty. The pressure transmitter readings allow classification of high pressure levels, no pressure or partial pressure. Similarly the flow transmitters identify readings of flow, no flow or partial flow.

2.4 *Fuel System Assumptions*

In modelling the fuel system various assumptions have been made. A blockage whether in a valve or a pipe assumes a complete blockage preventing any flow of fuel. Pipe rupture infers that the fuel will flow out of the rupture site and not along its intended path. A partial blockage (in a valve or pipe) refers to a partial stoppage of flow. A leak (in a valve or pipe) will result in some fluid loss yielding partial flow. For the analysis steady state operation of the system has been assumed as well as reliable sensor readings monitoring the system behaviour (with the issue of unreliable sensors discussed in section 5).

3 DIAGNOSTIC METHOD OVERVIEW

This paper considers the diagnostic application of the fault tree and digraph methods. Each method follows a set of steps described in sections 3.1 and 3.2.

3.1 *Fault Tree Diagnostic Method*

Fault Tree Analysis has been around as a reliability assessment technique since the 1970s. It is concerned with the analysis of failures and provides a diagrammatic description of the various causes of a specified system failure in terms of the failure of its components (Andrews & Moss, 2002). Utilising the method for fault diagnostics involves the following steps:

Step 1 - Construct fault trees for observable system deviations

The behaviour of the system can be monitored by sensors located at specific points. Fault trees are constructed to represent the failure modes at these locations. Non-coherent fault trees are constructed which include failure and success states of the components.

Step 2 – Determination of System Status

Compare the readings indicative of the current system behaviour with those that are expected given the mode of operation. Deviations are representative of fault(s) present.

Step 3 – Diagnostic Fault Tree Construction

Construct a top event structure from the sensor deviations identified in step 2. Combine all readings using an AND gate if more than one. Perform analysis to obtain potential causes of failure.

Step 4 – Consistency Verification

Check the potential causes of system failure obtained in step 3 against the sensors reading true to the operating mode. Any potential causes of failure that could cause these true sensor readings to be false can be removed.

Step 5 – Fault Cause Ranking

In the instance of multiple fault cause options importance rankings can be used to determine the most likely cause of failure.

3.2 *Digraph Diagnostic Method*

Digraphs (Andrews & Morgan 1986) can be used within engineering applications to represent the interrelationships between the process variables. These variables include measures such as temperature, mass flow and pressure. Nodes (or circles) in the diagram are used to represent the process variables and edges (lines) are used to represent the interconnections, i.e. positive/negative influences. Nodes also represent component failure modes, whereby a signed edge connecting a failure mode node to a process variable node indicates the disturbance which the failure mode can cause. A simple digraph is illustrated in Figure 2.

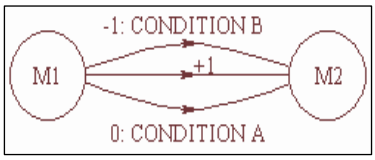

Figure 2. A Simple Digraph Representation

The process variables in Figure 2 are the mass flow at location 1 (M1) and the mass flow at location 2 (M2). The relationship between the two is reflected by the three edges. M1 is the independent variable whilst M2 is the dependent variable since a directed edge connects M2 to M1. The edge with a gain of +1 is a normal edge since this represents the relationship which is usually true. The second and third edges are conditional edges since their relationship is only true whenever the condition represented by ‘:’ exists. It must be noted that only one edge is true at any one time.

Process variable deviations and disturbances (Kohda & Henley 1988, Andrews & Brennan 1990) within digraphs are expressed as one of five discrete values: +10, +1, 0, -1, -10, representing respectively; large high, small high, normal, small low and large low. An unexpected process deviation within a system is represented by 'highlighting' the respective node in the digraph. Subsequent propagation of the deviation through the system is represented by marking all of the nodes which were affected by the initial highlighting.

To utilize the method for diagnosis initially the digraph of the system must be constructed. The steps for this process are:

Step 1 - System Definition
Define system to be analysed and list all component failures.

Step 2 – System Unit Classification
Separate the system into sub-units and identify and classify control loops, if present.

Step 3 – Diagraph Unit Model Development
Generate digraph models for the sub-units taking into consideration all process variable deviations which could have an effect on the variables in the model. Also consider the extent of the effect the process variable deviations may have on the system with regards to assigning discrete values to the deviations.

Step 4 – System Diagraph Formation
Form system digraph model by connecting common variables from the sub-unit models.

Once constructed the system digraph model can be used for finding the fault cause(s) by:

Step 5 - Identify Deviations
Compare actual and expected system behaviour.

Step 6 - Flag Non-deviating
Identify the non-deviating sensor nodes on the digraph.

Step 7 - Back-trace
Perform diagnosis from noted transmitter deviations to flagged non-deviated nodes or until no further back tracing can be carried out.

4 APPLICATION OF DIAGNOSTIC METHODS

4.1 *Actual System Operating Behaviour*

In using both methods deviations are considered from the normal expected operating behaviour of the system. In the active mode it is assumed that there would be flow out of the main and wing tanks into the collector tank, where fuel transfers to the engine. The expected sensor readings for the main tank would be that the level transmitter (LT0110) would indicate a level greater than the pump shut off requirement indicating fuel available for transfer. The flow transmitter (FT0100) which transfers fuel for draining would indicate no flow. The flow transmitter (FT0110) which monitors flow to the collector tank would register flow, and the pressure transmitters (PT0110/0120) would each register pressure (sensor codes are shown in figure 3).

The corresponding sensors on the wing tank would indicate the same respective readings. The readings for the Collector tank would also indicate required level, no flow to drain, flow to engine and pressure at both pressure transmitters.

The expected sensor readings can also be obtained for the other operational modes.

To illustrate within the paper the diagnostic process, the actual readings from all the sensors within the system have been assumed to indicate a deviation within the main tank.

The readings for this section are (with the deviated state in bold):

LT0110: >Pump Shut Off Level
FT0100: No Flow
FT0110: **No Flow**
PT0110/0120: Pressure

All other readings conform to expectation.

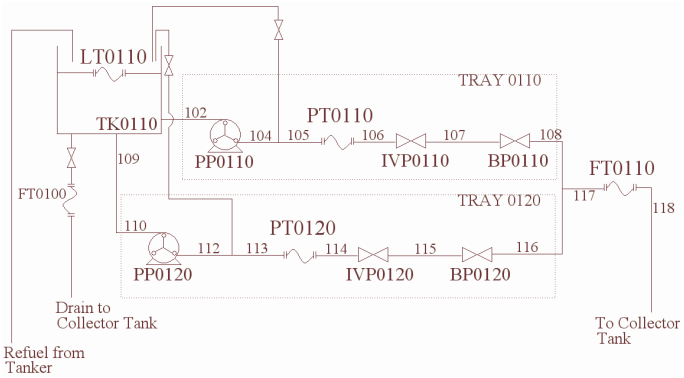

Figure 3. Main Tank

4.2 *Using The Fault Tree Method*

To utilise this method a fault tree is constructed to represent the causes of unexpected system behaviour. The inputs to this diagnostic tree depicting the actual system functionality are the fault trees for the necessary sensor failure modes (step 1). Considering the main tank, there would be three fault trees for the failure modes of the flow transmitter monitoring flow from the main tank to drain (FT0100), representing the causes of No Flow, Flow and Partial Flow. The same three fault tree failure modes would

be constructed for the flow transmitter monitoring the state of flow from the main tank to the collector tank (FT0110). Each pressure transmitter (PT0110 and PT0120) would have three fault trees representing the failure modes High Pressure, No pressure, Partial pressure.

Each fault tree for the sensor failure modes varies in size, with the largest having 55 gates and 90 events and the smallest fault tree having just 12 gates and 20 events. All fault trees contain failure and success events, therefore use AND, OR and NOT logic (referred to as non-coherent fault trees). The inclusion of the success events (or equivalent NOT logic) helps to remove failure causes that are not possible when more than one sensor failure mode are combined.

Given the actual behaviour of the system, deviations from the expected state is indicative of a fault or faults within the system. To establish the faults the causes are extracted by combining the individual faults trees constructed in step 1, representing the deviated readings, using AND logic.

From the assumed actual system behaviour (discussed in section 4.1) the deviated reading from the normal active behaviour involves the flow from the main tank to the collector tank (monitored by FT0110). The actual reading is No Flow, therefore the top event structure for the deviated state will involve just 'No Flow at FT0110'.

No flow at FT0110 is caused by either a failure immediately before the sensor, namely in the section of pipe labelled P117, or a failure on both lines 1 and 2 of the tank. When considering the failure at P117, it can fail blocked or ruptured. As the fault trees also consider the working states then if the pipe is ruptured it can not be blocked, partially blocked or leaking. If the pipe is ruptured it can not be blocked, partially blocked or leaking. Hence the intermediate gate combination will involve two intermediate input combinations, one will be the AND'ed combination of P117 blocked, NOT P117 ruptured, NOT P117 partially blocked and NOT P117 leaking. The other will be P117 ruptured, NOT P117 blocked, NOT P117 partially blocked and NOT P117 leaking AND'ed together.

A failure will occur on line 1 if there is a blockage or a rupture in P102, P104, P105, P106, P107, or P108. If P102 is blocked then it can not be ruptured, partially blocked or leaking, similarly if it is ruptured it can not be blocked, partially blocked or leaking. The same analogy can be made for the other five pipes (P104-108). The isolation valve, IVP0110, could be blocked, or failed closed, and NOT failed open, stuck, partially blocked or leaking. The back pressure valve, BP0110, could be blocked and NOT partially blocked or leaking, or the pump itself (PP0110) could have failed shut off and NOT failed mechanically, leaking or failed on.

Similarly a failure will occur on line 2 if there is a blockage or a rupture in P109, P110, P112, P113, P114, P115 or P116. They can not be ruptured, leaking or partially blocked if blocked. If the pipes are ruptured then they can not be blocked, partially blocked or leaking. The IVP0120 valve could be blocked or failed closed and NOT failed open, leaking or stuck. The back pressure valve BP0120 could be blocked and NOT partially blocked or leaking, or the pump (PP0120) could be shut off and NOT failed mechanically, leaking or failed on. The tank also could be the problem area having ruptured.

When analysing the fault tree using the standard qualitative procedures prime implicants are produced. These are combinations which include failure and success events. For example, one combination from 'No flow at FT0110' is: P102B.P109B.-P102F.-P102PB.-P102L.-P109F.-P109PB.-P109L where the – symbol means NOT that failure event. As the purpose of the diagnosis is to yield the failure events, a coherent approximation needs to be carried out (basically removing the success states) to yield the combinations of failure causes. Therefore the coherent approximation of the example prime implicant would be P102B.P109B. In total for this given system state there are a total of 292 failure causes for having No Flow at FT0110.

Information can be gained by considering those sensors that are true to the operating mode, hence reducing any causes from the list which can not be possible as they are functioning to permit non-deviating outcomes. Performing this consistency check results in 83 fault combinations. Two are single component failures, pipe 117 blocked (P117B) and pipe 117 ruptured (P117R). The remaining 81 combinations all involve the failure of two components together.

To try and establish the most likely cause of failure importance measures can be used. The Fussel-Vesely probabilistic measure of minimal cut set importance has been used in this research. Each potential failure cause combination (cut set) can be given a numerical rating, with the highest rating being deemed the most likely cause of failure. This value is calculated by evaluating the probability of cut set failure divided by the diagnostic tree probability of failure. For this example, the single order cut sets rank first and second, with the pipe rupture cause being ranked highest due to its higher probability of occurrence.

4.3 *Using The Digraph Method*

With the system defined and the component failure modes identified, the next step involves constructing the unit digraph models for the main, collector and wing tanks (step 3). Due to the inclusion of partial failure modes in the analysis a further two discrete values +5 and -5, representing moderate high and moderate low, are used to describe process variable deviations and the gains associated with the edges connecting failure modes.

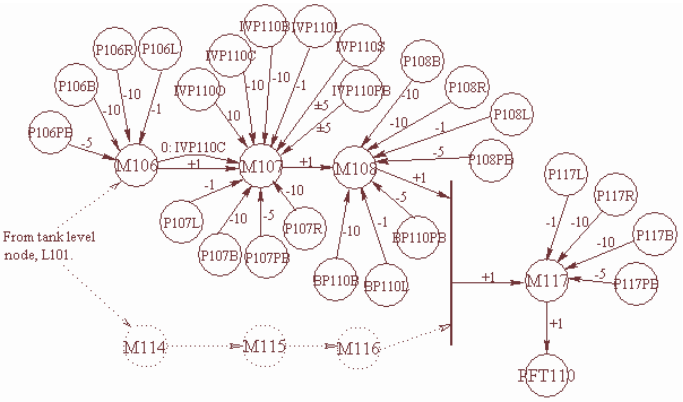

Figure 4: Part of Main Tank Digraph

The unit model digraph for the main tank is developed through a process of 'building-up' from the tank level node, L101. Two near identical branches extend from L101. These represent the flow of fluid from the tank through the peristaltic pumps, PP0110 and PP0120. The upper branch on the full digraph model encompasses mass flow (denoted M in the digraph nodes) along pipe 102 through to pipe referenced 108, representing the flow of fluid through the main tank line one of Figure 3. The mass flow section M106 to M108 is shown in figure 4. The lower branch of the full model depicts flow through line two of the main tank, encompassing mass flow from locations 109 to 116 (the part section from pipe 114, M114, to pipe 116, M116, is shown in Figure 4). Towards the end of each main tank line there is a powered isolation valve (IVP0110, IVP0120) and back pressure valve (BP0110, BP0120). If the powered isolation valves are closed by the operator then this would invoke a nullification of the relationship between the mass flows either side of the valve. Nodes M108 and M116 (mass flow at location 108 and 116) are connected though an 'AND' gate since a failure would have to occur in both main tank lines if no mass flow was to pass to the collector tank through pipes at locations 117 and 118. All of the mass flow nodes are positively dependant on the mass flow at the previous location and hence are connected by edges 'signed' +1. Mass flow also has a positive effect on the force powering the peristaltic pumps.

The rest of the digraph model for the main tank is built up in the same way. The unit model for this tank is constructed from 242 nodes, 43 process variables and 199 component failure modes (140 of these being pipe failures). The same process is carried out for the wing and collector tank models. The three individual units are connected via common nodes to form the full system digraph model (step 4 of the diagnostic process). In total there are 842 nodes; 151 are process variable nodes and 691 are component failure mode nodes. This completes the digraph construction steps.

The diagnosis phase involves back-tracing through the system digraph from a specific node which represents the location of the given deviation, if more than one deviation is experienced then back tracing commences at all points.

Given the actual system behaviour for the fuel system this deviates from the known operating mode of the system with flow at the flow transmitter FT0110. Hence, the diagnostic results obtained from the digraph are explained in the following steps:

1) Given the FT0110 flow deviation, back-tracing takes into consideration failure modes resulting in a large negative disturbance correlating with the situation of 'no flow' e.g. M117(-10).
2) From the non-deviating transmitter readings, the following parts of the digraph can be flagged: upper and lower branches incorporating PT0110 and PT0120, as well as the sections related to the level transmitter LT0110 and flow transmitter FT0100.
3) The direct component failure mode inputs into the node M117(-10) leads to the failure mode of pipe 117 being blocked or ruptured (P117B or P117R). Further back-tracing from M117(-10) leads to M116(-10) AND M108(-10).
4) Back-tracing past the 'AND' gate on the upper branch reveals failures leading to M108(-10). There are three failure modes which could lead to a large negative disturbance at node M108; pipe 108 being blocked or ruptured (P108B/R) and the block bleed valve BP0110 failing blocked (BP110B). Further failure modes are determined through following the fault propagation to node M106(-10). Back-tracing ceases at node M106 due to reaching the flagged section associated with PT0110.
5) Back-tracing past the 'AND' gate on the lower branch reveals failures leading to M116(-10). There are three failure modes which could lead to a large negative disturbance at node M116; pipe 116 being blocked or ruptured (P116B/R) and the block bleed valve BP0120 failing blocked (BP120B). Further failure modes are determined through following the fault propagation to node M114(-10). In a similar manner to the procedure

described in (4), back-tracing ceases at node M114 due to reaching the flagged section associated with PT0120.

The diagnostic results achieved through the process of back-tracing for the deviation in the actual readings are shown in Table 1.

Before 'AND' gate	P117B/R
OR	
Upper Branch	P108B/R, BP110B, P107B/R, IVP110C, IVP110B, P106B/R
AND	
Lower Branch	P116B/R, BP120B, P115B/R, IVP120C, IVP120B, P114B/R

Table 1. Faulty Scenario Diagnostic Results

For the given scenario it is possible that either a single fault or multiple fault may have led to the registered deviation; the diagnostic results confirm this. In total there are 83 failure mode options; 2 single order and 81 second order. Final human intervention, with the ability to call on engineering knowledge and experience will target the most probable failure modes. The list of failure modes can be further reduced by changing the operating mode of the system and comparing the causes for any registered sensor deviations noted in the two phases. In the case of multiple deviating sensors, the diagnostic results for each sensor are AND-ed together to determine the possible failure cause(s).

Through incorporating 'flagging' into the diagnostics process potential inconsistent failure mode results and anomalies are removed. This acts as a form of consistency check and removes the possibility for conflicting results to exist between non-deviating sensor readings and failure modes ascertained through back-tracing from deviating nodes.

5 DISCUSSION

5.1 *Overall Performance of the Methods*

The digraph and the fault tree approaches are noted as displaying a complementary perspective. Digraphs display the failure propagation route through a system whereas fault trees focus on a certain combination of events which can lead to the top event (noted deviation).

Both methods require diagnostic models (either a fault tree or a digraph) to be constructed prior to any analysis. In addition the similarities extend to requiring the difference to be calculated between actual system behaviour and that which is expected. With the large number of sensors throughout the whole system there is the potential for thousands of deviations from the expected behaviour. It has not been possible to test both techniques on all possible system state alternatives, however consideration of single, two failures and a collection of more than two failures has yielded encouraging results.

The main discussions on the fault tree method are in section 5.2 and for the digraph in section 5.3.

5.2 *Fault Tree Review*

To utilise the fault tree method requires the systematic breakdown of the causes of each failure mode for each sensor. The generation of each of these trees is the major task in using this method. As the number of sensors increases the number of fault trees required similarly increases. Having generated these trees the method for diagnosis is very straight forward and easy to implement. This issue of scalability could be a factor with more sensors because as the number of deviations increase the number of inputs in the diagnostic tree increases. Within the aircraft fuel system application this has not been a limiting factor.

The results obtained from the analysis of the fuel system have yielded viable fault causes, although several options have been produced. Importance measures have provided one means to be able to identify the most likely cause. The current research has not considered faulty sensor readings although a method of using other system parameters such as flow rate and rate of change of height have been identified as a means to locate unreliable sensors.

Direct application of the method discussed in the paper to diagnose faults when the system is operating dynamically may not be straight forward, and the consideration of time factors may need to be incorporated.

5.3 *Digraph Review*

Digraphs provide a clear representation of the relationships between the system variables as it closely reflects the physical structure of the system. To produce the model requires a thorough understanding of the system, however it can be developed from detailed engineering drawings. The full digraph for the application system is relatively large, however development is aided by the sub-unit divisions.

In terms of the diagnosis process the method of back tracing, using deviated and non-deviated variables, is very simple and can easily be automated within computer code. Flagging of non deviating sections removes the possibility of revealing inconsistent failure modes or anomalies in the fault diagnostic results. The inclusion of +/- 5 within the di-

graph has provided the ability to include partial failures into the analysis.

The limitations and extensions of the method firstly relate to the dynamic effects, although preliminary research investigations in this area have focussed on using change of height information, in conjunction with transmitter readings.

A mechanism to identify the actual cause(s) of any deviations is required to reduce the current output from the model. Investigations focus on using knowledge of past failures (if present) and weighting failure modes. Other issues to investigate are unreliable sensors and identification of these sensors, which is likely to include some form of time function. The issue of extendability to more complex systems seems plausible as even with large models they can easily be handled with modern computer systems. Also the technique is suited to handle control mechanisms and therefore provides flexibility to perform diagnosis on these types of system.

6 CONCLUSIONS

Both methods have produced realistic results for steady state behaviour. With no difference in predictive potential for this application system the digraph method seems the most efficient (as consistency checking is done within the approach). Further research is required in terms of dynamic behaviour and importance of sensor location to aid diagnosis.

Acknowledgements

The authors wish to thank the SEIC and BAE Systems for the information on the aircraft fuel system.

7 REFERENCES

Andrews, J. & Brennan, G. 1990. Application of the Digraph Method of Fault Tree Construction to a Complex Control Configuration. *Reliability Engineering and System Safety*, 28(3), pp. 357.

Andrews, J. & Morgan, J. 1986. Application of the Digraph Method of Fault Tree Construction to Process Plant. *Reliability Engineering*, 14(2), pp. 85.

Andrews, J. & Moss, T. 2002. *Reliability and Risk Assessment*. PEP.

Henning, S. & Paasch, R. 2000. Diagnostic Analysis for Mechanical Systems. *Proceedings of the ASME Design Engineering Technical Conferences*, 4, pp. 391.

Hurdle, E., Bartlett, L. & Andrews, J. 2005. System Fault Diagnostics Using Fault Tree Analysis, *Proceedings of the 16th Advances in Reliability Technology Symposium.*

Iverson, D. & Pattersine-Hine, F. 1995. Advances in Digraph Model Processing Applied to Automated Monitoring and Diagnosis. *Reliability Engineering and System Safety*, 49(3), pp. 325.

Kohda, T. & Henley, E. 1988. On Digraphs, Fault Trees and Cut Sets. *Reliability Engineering and System Safety*, 20(1), pp. 35.

Novak, F., Žuzek, A. & Biasizzo, A. 2000. Sequential Diagnosis Tool. *Microprocessors and Microsystems*, 24(4), pp. 191.

Pattipati K. R. and Alexandridis M. G. 1990. Application of Heuristic Search and Information Theory to Sequential Fault Diagnosis, *IEEE Transactions on Systems, Man and Cybernetics*, 20 [4] 872-887.

Price, C. 1997. AutoSteve: Electrical Design Analysis. *Colloquium Digest – IEE*, 338(4).

Price, C. & Taylor, N. 1997. Multiple Fault Diagnosis from FMEA, *Proceedings from the National Conference on Artificial Intelligence*, pp1052.

Shakeri M., Raghavan V., Pattipati K. R. and Patterson-Hine A. 2000. Sequential Testing Algorithms for Multiple Fault diagnosis, *IEEE Transactions on Systems Man and Cybernetcis - Part A: Systems and Humans*, 30 [1] 1-14.

Venkatasubramanian, V., Rengaswamy, R., Yin, K. & Kavuri, S.N., 2003. A Review of Process Fault Detection and Diagnosis Part I: Quantitative Model-based Methods. *Computers and Chemical Engineering*, 27(3), pp. 293.

Yangping Z., Bingquan Z. and Dong Xin W. 2000. Application of Genetic Algorithms to Fault Diagnosis in Nuclear Power Plants, *Reliability Engineering and System Safety*, 67:153-160.