This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Integrated system fault diagnostics utilising digraph and fault tree-based approaches

PLEASE CITE THE PUBLISHED VERSION

PUBLISHER

© Elsevier

VERSION

AM (Accepted Manuscript)

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Bartlett, L.M., Emma E. Hurdle, and Emma M. Kelly. 2009. "Integrated System Fault Diagnostics Utilising Digraph and Fault Tree-based Approaches". figshare. <https://hdl.handle.net/2134/4342>.

This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) 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/>

Integrated System Fault Diagnostics Utilising Digraph and Fault Tree Based Approaches

L.M. Bartlett, E.E. Hurdle & E.M. Kelly
Aeronautical and Automotive Engineering Department,
Loughborough University,
Loughborough, UK.
L.M.Bartlett@lboro.ac.uk
t:+44(0)1509 227276
f:+44(0)1509 227275

ABSTRACT:

With the growing intolerance to failures within systems, the issue of fault diagnosis has become ever prevalent. Information concerning these possible failures 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. In addition, a diagnostic capability is required in real time and for changeable system functionality. This paper focuses on two approaches which have been developed to cater for the demands of diagnosis within current engineering systems, namely application of 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. The procedural guidelines are discussed for each method, with an experimental aircraft fuel system

used to test and demonstrate the features of the techniques. The effectiveness of the approaches are compared and their future potential highlighted.

1 INTRODUCTION

To maximise the operational functionality of any system or the effectiveness of any mission it is imperative that failures are detected as quickly as possible. The ability to diagnose a fault when it occurs is the first step to minimising this failure disruption time. Missions can be altered, systems reconfigured and spares ordered to enable the successful use of the resultant operative state.

Early methods dealing with diagnostic capability focused on identifying faults at a specific point in time using a series of testing procedures [1, 2]. A symptom – fault relationship is evaluated, where a series of tests are used to filter to the actual fault cause. These approaches have been found to be effective in identifying single faults and also work well as an offline evaluation mechanism, i.e. 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, the characteristics associated with modern day systems require real time diagnosis and to incorporate both adaptability and identification of multiple faults [3]. With systems and missions often involving changing conditions and operational modes, adaptability is key to perform diagnosis for the full mission or system life.

To accommodate these system characteristics extensions to the early testing procedures have been developed [4], in addition such tools as genetic algorithms [5] have been implemented, both with limited success. More recent approaches include using failure modes and effects analysis [6, 7], fault tree analysis [8, 9] and a

combination of both [10]. The successfulness of these methods has been variable as the system complexity increases. The method of digraphs has been used for limited multiple failures [11] 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 approaches. The differences between [8] and [9] are that the best approach laid out in these papers is extended to a larger system and the work considers system dynamics using flow pattern recognition. The approach can still obtain multiple failures and checks for consistency. With regards to reference [11], this paper considers process variables not just component failure modes, and also process variable effects are considered. Reference [11] uses a more prognosis based approach for identifying weak links whereas this research using the method of back tracing. The evaluation of both methods is based on the application to an aircraft fuel rig system. The methods include the capability to evaluate multiple fault causes from a given system deviating state, inclusion of transient effects and analysis of dynamic system behaviour is considered, and both are adapted to include a form of consistency check for the results obtained. The work has the added originality of being applied to an experimental simulator which aids the validation of the results.

The remaining sections of the paper are divided into; section 2 explains each of the individual diagnostic methods; section 3 reviews the application fuel system in detail; section 4 considers the results obtained from the diagnostic methods when applied to the fuel rig for steady state and dynamic conditions; section 5 reviews each method, with section 6 reporting the overall conclusions to the research.

2 THE DIAGNOSTIC METHODS

This paper considers the diagnostic application of the fault tree and digraph methods. Details of the fundamentals of each procedure are stated, with the similarities involving the comparison of actual and expected system behaviour. Application of these steps to an aircraft fuel system is detailed in section 4.

2.1 *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 [12]. Utilising the method for fault diagnostics involves the following steps:

Step 1 – Component and Sensor Identification

Identify the components contained within the system and the failure modes of each. Identify the sensors contained or needed within the system to be used to monitor system behaviour.

Step 2 - Construct fault trees for observable system deviations

The behaviour of the system can be monitored by sensors located at specific points, i.e. flow meters. Fault trees are constructed to represent the failure modes at these locations, i.e. High Flow. Non-coherent fault trees are constructed that include failure and success states of the components, which removes inconsistencies between working and failed components. An example is given in Figure 1 to represent unwanted high flow at a valve (valve 1, shown in Figure 2). Using not logic one cause is because the valve has

failed open, and hence it cannot fail closed. The valve has an inlet pipe and an outlet pipe (pipes 1 and 2), in order for flow to occur water must be available from the main supply and able to pass through the pipes. The necessary success events have been included in the right hand branch.

Step 3 – 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 faults present.

Step 4 – 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 there are more than one. Perform a standard qualitative analysis to obtain potential causes of failure.

Step 5 – 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 6 – Fault Cause Ranking

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

2.2 Digraph Diagnostic Method

Digraphs [13] can be used within engineering applications to represent the interrelationships between the process variables, such as temperature, mass flow and pressure. A diagram is constructed where nodes (or circles) 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 representation of a valve system unit (Figure 2) is illustrated in Figure 3. The valve unit is comprised from three components; namely, Pipe 1, Pipe 2 and Valve 1.

The respective valve unit digraph depiction is formed by taking the process variable mass flow into consideration. The nodes M1 and M2 represent mass flow at Pipes 1 and 2 respectively. The relationship between the two nodes 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. For the valve unit case, this symbolises the fact that under normal circumstances mass flow in Pipe 1 has a positive effect on mass flow in Pipe 2 (i.e. valve open). The second and third edges are conditional edges since their relationship is only true whenever the condition represented by ‘:’ exists. For example, the relationship between the two nodes is nullified should Valve 1 be closed (Condition A). It must be noted that only one edge is true at any one time.

Process variable deviations and disturbances [14, 15] 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.

There are two phases to the diagnosis, initially the digraph must be constructed for the system under analysis, then this model is used to carry out the fault identification. The steps for digraph construction are:

Step 1 & 2 - System Definition and Unit Classification

Define system to be analysed and list all component failures. Separate the system into sub-units and identify and classify control loops, if present.

Step 3 – Digraph 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 Digraph 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 application of steps 5 to 7:

Step 5 - Identify Deviations

Compare actual and expected system behaviour.

Step 6 - Flag Non-deviating Nodes

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.

3 FUEL SYSTEM

3.1 *System Architecture*

The system used to test the capability of the fault tree and digraph diagnostic methods is representative of an aircraft fuel system. It is an experimental fuel rig, illustrated in Figure 4, where water is used instead of aviation fuel. The purpose of the system is to provide an adequate amount of clean fuel at the required pressure to the engines during all phases of flight.

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 (comprised of the main, wing and collector) from the engine tank (representative of refuelling). 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.

3.2 Component Failure Modes

There are 43 different component failure modes considered in the analysis, which may affect the functionality of the fuel rig system. Table 1 illustrates these failure modes. Each component failure mode is allocated a code which contains the relevant component identification number. In table 1 these replace ‘***’. The majority of the failure modes (30) are associated with one of six valve categories. 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. 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.

3.3 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. Table 2 illustrates the specific sensors associated with each of the tank sections.

3.4 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 (the consideration of dynamic behaviour is addressed in sections 4.2 and 4.3).

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 (>PSO) requirement indicating fuel available for transfer. The flow transmitter (FT0100) in the fuel drain line 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 (the main tank schematic with sensor codes is shown in Figure 5).

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.

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.

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', as shown in Figure 6.

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 cannot be blocked, partially blocked or leaking. If the pipe is ruptured it cannot be blocked, partially blocked or leaking. Hence the intermediate gate combination will involve two intermediate input combinations, one will be the ANDed combination of P117 blocked with NOT the other failure modes for P117, and the other will be P117 ruptured with NOT P117s other failure modes ANDed 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.-P102R.-P102PB.-P102L.-P109R.-P109PB.-P109L where the – symbol means NOT that failure event. This combination involves eight pipe failure modes (referenced as P then three numbers corresponding to the pipe section). The modes of failure for these pipes are either blocked (B), partially blocked (PB), leaking (L) or ruptured (R). 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 Fussell-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.

In order to improve the accuracy of the results the dynamics of the system need to be taken into account. The diagnostic process follows the same steps as illustrated for the steady state case, although step 2 is modified slightly. In this step comparison of actual and expected behaviour occurs via observation of patterns from the sensors over time rather than specific values. It is only the shape of the sensor reading patterns that need to be identified. Fluctuations or noise is permitted within a certain boundary in order to account for small discrepancies in the results..

Considering the whole flight phase for certain operating modes has shown that the number and complexity of patterns is extremely large to deal with effectively. In order to overcome this, these modes have been split into 'sub-modes' that depend upon the level in the collector tank. For instance the ACTIVE operating mode has been split into six sub-modes, each indicating expected behaviour of the system for the given level in the collector tank. Table 3 shows typical patterns for the three tanks with accompanying water levels for one phase of the active mode operation (RL refers to required level of water and T1 the level where additional fluid is required

from the collector tank). Initially patterns are compared for the individual tank units, along with the water level. The tank or tanks identified as inconsistent with the expected readings are then examined in more detail. Here patterns for the sensors located in the deviating tank sections are compared. Step 3 then continues with the combination of relevant fault trees for the differing patterns.

To illustrate by extending the steady state faulty scenario of No Flow at FT0110, the outflow from the main tank, with the added knowledge of evidence of a constant level in the tank removes invalid fault possibilities. Deviations would be evident in the patterns from the main tank. From the previous investigation potential failure causes included possible ruptures. However, the information from the level sensor contradicts this. Combining the fault trees for the deviated sensor readings within the main tank together with those working successfully yield 37 potential failures.

4.3 Using The Digraph Method

With the system defined and the component failure modes identified, the next phase in the procedure involves constructing the unit digraph models for the main, collector and wing tanks (step 3). Part of this process involves the allocation of appropriate process variable deviations. The significance of these are:

- Signed edges in digraphs are allocated a numeric value so as to indicate a more precise relationship.
- The value is considered in terms of a magnitude with regards to large positive or small positive for example.

- In this manner it aids the diagnostic process in determining more specific component failure mode data when back-tracing from known deviating nodes (since sensor deviations are classified using similar discrete values e.g. -10 represents status no flow if expected flow).
- To enhance the specificity of the relationships between variables (i.e. to differentiate between normal flow (usually assigned +/-1), high flow (usually assigned -/+10) and partial flow, in addition to the standard -10, -1, 0, 1, 10, a further two discrete values +5 and -5, representing moderate high and moderate low, are used.

Figure 7 details the end portion of the main tank section incorporating two powered isolation (IVP0110/ IVP0120) and back pressure valves (BP0110/ BP0120). The flow transmitter FT0110 is also noted. Figure 8 illustrates the respective section of the main tank digraph.

The unit 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 main tank through the peristaltic pumps, PP0110 and PP0120. The upper branch encompasses mass flow from location 102, referred to as M102, to mass flow at location 108, M108. It represents the flow of fluid through line one in the main tank.

The lower branch depicts flow through line two of the main tank, encompassing mass flow from locations 109 to 116. 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 flow nodes either side of the valve, as represented by the conditional signing of the arc ‘0:

IVP110C' connecting nodes M106 and M107 in Figure 8. Nodes M108 and M116 (mass flow at locations 108 and 116) are connected through an 'AND' gate since a failure would have to occur in both main tank lines if no mass flow were to pass to the collector tank through pipes at locations 117 and 118. All mass flow nodes are positively dependent 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 unit model for the main tank is constructed from 242 nodes, 43 process variables and 199 component failure modes (140 of these being pipe failures). A similar digraph generation process is conducted for the wing and collector tank models. The three individual units are connected via common nodes to complete the construction of the full system digraph model (step 4 of the diagnostic process). In total there are 842 nodes; of which there are 151 process variable nodes and 691 component failure mode nodes.

The diagnosis phase involves back-tracing through the system digraph from a specific node which represents the location of the given deviation. For cases encompassing more than one deviation, the back-tracing procedure then commences from all nodes that register a disturbance. The results for the individual deviating nodes are ANDed together in order to yield possible failure combinations.

The retrieved system behaviour for the fuel rig system deviates from the known operating mode conditions through the registering of 'no flow' at the flow transmitter FT0110. The diagnostic results obtained from the digraph are thus explained:

- 1) Given the flow deviation at FT0110, back-tracing takes into consideration failure modes resulting in a large negative disturbance. A large negative disturbance correlates with the situation of 'no flow' e.g. M117(-10).
- 2) From the non-deviating transmitter readings, the following segments of the main tank digraph can be flagged: upper and lower branches incorporating the pressure transmitters PT0110 and PT0120, shown in figure 5, as well as the sections related to the level transmitter LT0110 and flow transmitter FT0100.
- 3) From the component failure mode nodes directly related to node M117, two failure modes are highlighted as leading to a large negative disturbance in mass flow at location 117. These are 117 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 blocked or ruptured (P108B/R) and the back pressure valve BP0110 blocked (BP110B). Further failure modes are determined through following the fault propagation to nodes M107(-10) and 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 blocked or ruptured (P116B/R) and the back pressure valve BP0120 blocked (BP120B). Further failure modes are determined through following the fault propagation to nodes M115(-10) and 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 from the registered deviating node in the main tank digraph are illustrated in Table 4. 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 ANDed together to determine the possible failure cause(s).

Taking into consideration dynamic system effects enables a more thorough system analysis. The suggested strategy is to analyse system behaviour at frequent intervals in order to perform diagnostics and therefore identify if the system has shifted from its normal operating mode. This involves monitoring the fuel rig system from data retrieved at a set sampling rate and subsequently determining if the system is in an abnormal scenario. There are now a number of different expected readings in the active mode determined by the level of water in the tank, which ultimately affects from which tank fuel may be distributed. The dynamic effects of faults are investigated through examining the tank levels, in particular the rate of change in levels.

Considering the same dynamic example as used for the fault tree method, based on the faulty scenario utilised in section 4.1, where it is assumed that the deviating transmitter readings remain the same between sampling intervals in addition to a recorded static tank level. The back-tracing procedure is identical to that previously described. The rate of change in height of the main tank level is used to distinguish between and hone-in on failures that may be the cause for the given deviation. The zero rate of change in tank level indicates the occurrence of faults incorporating blockages or closures. Conversely, a negative rate of change along with ‘no flow’ at FT0110 would suggest rupture faults. Taking the rate of level change into consideration generates 37 failure combinations; one first order and 36 second order.

Taking into account dynamic effects for the same faulty scenario allows for a reduction in the list of possible failure combinations. When comparing the diagnostic results from the previous section with the dynamic results it is noted that the number of fault causes listed is more than halved.

The use of the Fussell-Vesely measure of importance can also be used, like in the fault tree approach, to hone-in further on the most probable fault cause from the list of possible options produced.

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, in addition the derivation of expected patterns of behaviour. The generation of each of the fault 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 and patterns 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. With the modular approach applied under dynamic conditions (looking at the patterns at system level then sub-unit level then honing in on deviating sections) the issue of scalability is reduced as each stage is of a manageable size.

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 seems relatively straightforward by the use of considering patterns of behaviour over time. The difficult area is perhaps identifying the units for evaluation at each stage of pattern recognition. For this fuel rig example the division has been easily achieved.

5.3 Digraph Review

Digraphs provide a clear representation of the relationships between the system variables due to their close reflection of the physical structure of the system under analysis. 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; nevertheless development is aided by the sub-unit divisions.

With regards to the fault diagnostics process, the method of back tracing using deviating and non-deviating variables, is relatively straightforward 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 digraph has provided the ability to include partial failures into the analysis.

The flagging process is easily extended to consider transient effects with comparison for specific active mode values depending on the levels of fuel in the tank. Incorporating details of the rate of change in the tank level helps to correctly identify fault causes.

The use of importance measures to determine the most likely fault cause for a given deviation helps to hone-in on the most probable fault cause. Current focus is based on investigating a mechanism to further identify the actual cause(s) of any registered deviations through consulting data documented by technical personnel in maintenance logs.

The issue of extending the method to more complex systems is plausible, as even large models can easily be handled by modern computer systems. The technique is also suited to handling control mechanisms and therefore provides the flexibility to perform fault diagnostics of complex systems.

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) under these conditions. The research for dynamic behaviour has illustrated a modular approach can be used during the application of the fault tree approach which means that the problem is solved in manageable step sizes, for the digraph method use of rates of change are applied to extend the original steady state procedure. Both methods are straightforward to apply once the models are created. The techniques have tackled the characteristics of multiple faults, transient and dynamic behaviour

and considered consistency check for validation of results. The importance of sensor location to aid diagnosis is an area which may benefit both methods.

Acknowledgements

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

7 REFERENCES

- [1] Novak, F., Žuzek, A. & Biasizzo, A. 2000. Sequential Diagnosis Tool. *Microprocessors and Microsystems*, 24(4), pp. 191.
- [2] 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.
- [3] 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.
- [4] 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 Cybernetics - Part A: Systems and Humans*, 30 [1] 1-14.
- [5] 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.

- [6] Price, C. 1997. AutoSteve: Electrical Design Analysis. *Colloquium Digest – IEE*, 338(4).
- [7] Price, C. & Taylor, N. 1997. Multiple Fault Diagnosis from FMEA, *Proceedings from the National Conference on Artificial Intelligence*, pp1052.
- [8] Hurdle, E., Bartlett, L. & Andrews, J. 2005. System Fault Diagnostics Using Fault Tree Analysis, *Proceedings of the 16th Advances in Reliability Technology Symposium*.
- [9] E E Hurdle, L M Bartlett, J D Andrews, “System Fault Diagnostics Using Fault Tree Analysis”. *Journal of Risk and Reliability, Part O of the Proceedings of the IMechE*, Vol. 221, No. 1, p43-55.
- [10] Henning, S. & Paasch, R. 2000. Diagnostic Analysis for Mechanical Systems. *Proceedings of the ASME Design Engineering Technical Conferences*, 4, pp. 391.
- [11] 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.
- [12] Andrews, J. & Moss, T. 2002. *Reliability and Risk Assessment*. PEP.
- [13] Andrews, J. & Morgan, J. 1986. Application of the Digraph Method of Fault Tree Construction to Process Plant. *Reliability Engineering*, 14(2), pp. 85.
- [14] Kohda, T. & Henley, E. 1988. On Digraphs, Fault Trees and Cut Sets. *Reliability Engineering and System Safety*, 20(1), pp. 35.
- [15] 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.

Figure 1. Example Non-Coherent Fault Tree

Figure 2. Valve Example

Figure 3. Simple Digraph Representation

Figure 4. Fuel Rig Schematic

Code	Component Failure	Code	Component Failure
TK***L	Tank leakage	TK***R	Tank rupture
P***L	Pipe leaks	P***B	Pipe blocked
P***R	Pipe ruptured	P***PB	Pipe partially blocked
PP***O	Peristaltic pump failed on / too high	PP***L	Pipe in peristaltic pump leaks
PP***S	Peristaltic pump failed off	PP***M	Mechanical failure of peristaltic pump
CP***O	Centrifugal pump failed on	CP***S	Centrifugal pump failed off
PSV***B	Pressure relief valve blocked	CP***L	Centrifugal pump leaks
PSV***PB	Pressure relief valve partially blocked	PSV***S	Pressure relief valve stuck (intermediate)
PSV***L	Pressure relief valve leaks	PSV***O	Pressure relief valve opened at incorrect pressure
IVP***B	Powered isolation valve blocked	PSV***C	Pressure relief valve closed at incorrect pressure
IVP***PB	Powered isolation valve partially blocked	IVP***S	Powered isolation valve stuck (intermediate)
IVP***L	Powered isolation valve leaks	IVP***O	Powered isolation valve failed open
CK***B	Check valve blocked	IVP***C	Powered isolation valve failed closed
BP***L	Pressure regulating valve leaks	CK***PB	Check valve partially blocked
BP***B	Pressure regulating valve blocked	CK***L	Check valve leaks
BBV***B	Block bleed valve blocked	BP***PB	Pressure regulating valve partially blocked
BBV***L	Block bleed valve leaks	BBV***O	Block bleed valve failed open
TVL***L	Reconfiguration valve leaks	BBV***C	Block bleed valve failed closed
IV***O	Drain valve failed open	TVL***PB	Reconfiguration valve partially blocked
IV***C	Drain valve failed closed	TVL***B	Reconfiguration valve blocked
IV***L	Drain valve leaks	IV***PB	Drain valve partially blocked
IV***B	Drain valve blocked		

Table 1. Fuel Rig System Component Failure Modes

Tank Section	Level Transmitter	Flow Transmitter	Pressure Transmitter
Main	LT0110	FT0100 (Drain route)	PT0110 (Feed line one)
	-	FT0110 (Tank feed line exit)	PT0120 (Feed line two)
Wing	LT0210	FT0200 (Drain route)	PT0210 (Feed line one)
	-	FT0210 (Tank feed line exit)	PT0220 (Feed line two)
Collector	LT0310	FT0300 (Drain route)	PT0310 (Feed line one)
	-	FT0310 (Tank feed line exit)	PT0320 (Feed line two)
Engine	LT0410	FT0400 (Refuel line exit)	-

Table 2. Fuel Rig System Sensor Locations

Figure 5. Main tank schematic showing sensors and main components

Figure 6. Fault tree representing No Flow at FT0110

	MAIN FT0110	MAIN LEVEL LT0110	WING FT0210	WING LEVEL LT0210	COLLECTOR FT0310	COLLECTOR LEVEL LT0310
ACTIVE1

Table 3. Tank Level Dynamic Sensor Patterns

Figure 7. Section of the Main Tank

Figure 8. Section of the Main Tank Digraph

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 4. Faulty Scenario Diagnostic Results