Enhanced diagnosis of faults using the digraph approach applied to a dynamic aircraft fuel system

Enhanced diagnosis of faults using the digraph approach applied to a dynamic aircraft fuel system

E M Kelly and **L M Bartlett***
Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, Leicestershire, UK

The manuscript was received on 1 October 2007 and was accepted after revision for publication on 5 August 2008.

DOI: 10.1243/1748006XJRR119

Abstract: Malfunctions within commercial aircraft can considerably increase both the financial cost of downtime and the disruption caused to passenger travel. For this reason prompt detection, diagnosis, and rectification of faults is imperative to the successful operation of such a system. In this paper the fault diagnostic problem is tackled based on the application of the digraph procedure. Digraphs model the information flow, and hence fault propagation, through a system. A computational method has been successfully developed to conduct the fault diagnostics process and produce a list of the fault combinations determined. The scope of the method has been demonstrated by consideration of two modes of operation to the application of a commercial aircraft fuel system, namely that of a Boeing 777. In addition the paper highlights the contribution of the development of a reduction method to enhance the likelihood of identifying the possible failure causes in three ways from different viewpoints. The three methods provide the option of determining the component at fault, the most probable failure mode cause, and also evidence for a particular component fault.

Keywords: fault diagnostics, digraphs

1 INTRODUCTION

The occurrence of failures within a system can cause disruption to the operational stability. Fault diagnosis has therefore become a primary objective in engineering applications. It is concerned with the isolation of underlying causal faults that can lead to an observable effect in a monitored process. Effective detection of system faults decreases downtime and consequently enhances operational stability [**1**].

Traditional approaches employed to identify faults involved using testing algorithms to detect single failures [**2**, **3**]. In using this approach, prospective faults are highlighted through the running of a series of tests at a particular point in time. The tests are composed of symptoms that are related to specific system faults. The effectiveness of the method has been proven when determining single faults in a system with a known period of inactivity. Difficulties are noted when considering the complexities of multiple fault combinations. In an effort to address the diagnosis of multiple faults, extensions to the sequential testing technique have been developed and implemented [**4**].

Some recent approaches have used reliability assessment tools such as failure modes and effects analysis (FMEA) [**5**, **6**] and fault tree analysis [**7**]. Attempts have been made to automate the FMEA process and increase its effectiveness through decreasing the time required for analysis. A different method proposes translating the information contained in a network of interconnected fault trees into FMEA-style tables [**8**]. Variability in the performance of these methods is noted with increased system complexity.

Digraphs, also known as signed directed graphs [**9**, **10**], illustrate specific fault propagations through a system. They are a type of causal model, clearly representing the cause and effect behaviour within a system. Causal models can be employed in fault diagnosis to reason about the behaviour of processes under normal and abnormal conditions [**11**].

**Corresponding author: Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, Leicestershire LE11 3TU, UK. email: L.M.Bartlett@lboro.ac.uk*

The characteristics associated with modern day systems require fault diagnosis to incorporate both adaptability and identification of multiple faults [**12**]. Modern systems are normally required to operate in more than one mode. An ideal diagnostic procedure would therefore incorporate an adaptable scope.

The research is centred on model-based diagnosis which uses models of a device or system as a basis for generating possible solutions for a given problem. A model indicating the expected behaviour of the system under a given set of operating conditions is created. Retrieved readings from the system are then compared with the model in order to reveal noted deviations, if present. It is assumed that registered deviations indicate the presence of a failure. Diagnosis is performed as a means for locating and determining the potential causes of the registered deviation. A number of different types of models are utilized within model-based diagnostic systems [**13**]. These include, to name a few, simple dependency, state-based, process, and causal models. A simple dependency model illustrates the fact that the correct working of one component depends on a number of others; a tree of dependencies is created with the most important components at the top of the tree. With regards to state-based models, systems may be characterized as a set of states; these states are linked by transitions in order to illustrate their possible movement within the application. Process models contain modules that can be linked in order to describe the system behaviour. This is useful within systems where the processes that are occurring are the most important feature. Causal models explicitly represent the behaviour of the complete system or device. Model-based diagnosis is most effective when different devices are composed of the same components. The user is required to determine which part of the system, be it physical components or system processes, are to be modelled. This paper applies a fault diagnostics strategy to the fuel system of a Boeing 777-200 aircraft. Thus, given the practical application and process variables under consideration, digraphs are used to model the system. The diagnosis procedure is then based on the system digraph.

This research work extends the research from reference [**14**]. Here the method is applied to an actual system, thus demonstrating the issue of scalability. Explanation of the system considered is given in section 2. In order to address the issue of adaptability, identified in reference [**14**] as an avenue of further investigation, diagnosis for two modes of operation of the system, engine feed and pressure refuel, are discussed. The procedure, involving model construction and diagnosis itself, is demonstrated, and the results yielded through automating the fault diagnostics process are reviewed in sections 3 and 4. Additional enhancements involve a revision of the 'honing-in' technique. These methods for honing in on the most probable component at fault as well as the specific failure mode of the component from the complete list of fault causes are discussed in section 5. The diagnostic program in this paper takes dynamic data into consideration and performs automatic consistency checks between both consecutive transmitter readings and between possible failure modes and associated transmitter indications. The dynamic aspect allows the modification of the entire digraph structure depending on its operational phase, thus allowing a greater scope for diagnosis. Final conclusions of the research are given in section 6.

2 AIRCRAFT FUEL SYSTEM

2.1 System design

The Boeing 777-200 is a twinjet aircraft that entered into revenue service in the middle of 1995. Fuel is stored in three tanks: the left main, centre, and right main. A surge tank is situated outboard of each main tank, the function of which is to temporarily hold fuel that flows owing to aircraft turns, thermal expansion, or overfilling. The 777-200 fuel system can hold a total of 117 400 : 35 200 l in each main tank and 47 000 l in the centre tank. Figure 1 provides an illustration of the left side of the Boeing 777-200 fuel system. The right side exhibits a similar structure. The engine feed operating mode is the primary phase considered in this analysis, with a second mode of pressure refuel, which incorporates a control aspect, also investigated.

2.2 System operating modes

2.2.1 Engine feed

The main purpose of the engine feed operating mode is to supply fuel to the engines from the main and centre tanks. Six powered fuel pumps supply fuel to the engines. The engine feed operating mode is subdivided into five operational phases. The five phases represent the manner in which engine feed can be conducted.

- Phase one: fuel is pumped from the centre tank into the engine feed manifold by the jettison/override pumps.
- Phase two: once the centre tank is nearly empty, fuel is pumped from the main tanks into the engine feed manifold by the main tank boost pumps.
- Phases three and four: fuel can be transferred from one wing to the other by opening one of the cross-feed valves and shutting off the pumps on the side to which fuel is being transferred.

- Phase five: for cases whereby the fuel pumps are switched off and the cross-feed valves are closed, engine feed can occur through suction via the suction bypass valves in the main tanks.

A mixture of sensors and switches are utilized in the fuel system to provide system information regarding flow, pressure, and tank levels. Those used for the engine feed phase are described in Table 1 (in the column headed 'Variable').

2.2.2 *Pressure refuel*

The main purpose of the pressure refuel operational phase is to transfer fuel from the refuel adaptors to the airplane tanks. The refuel system is operated

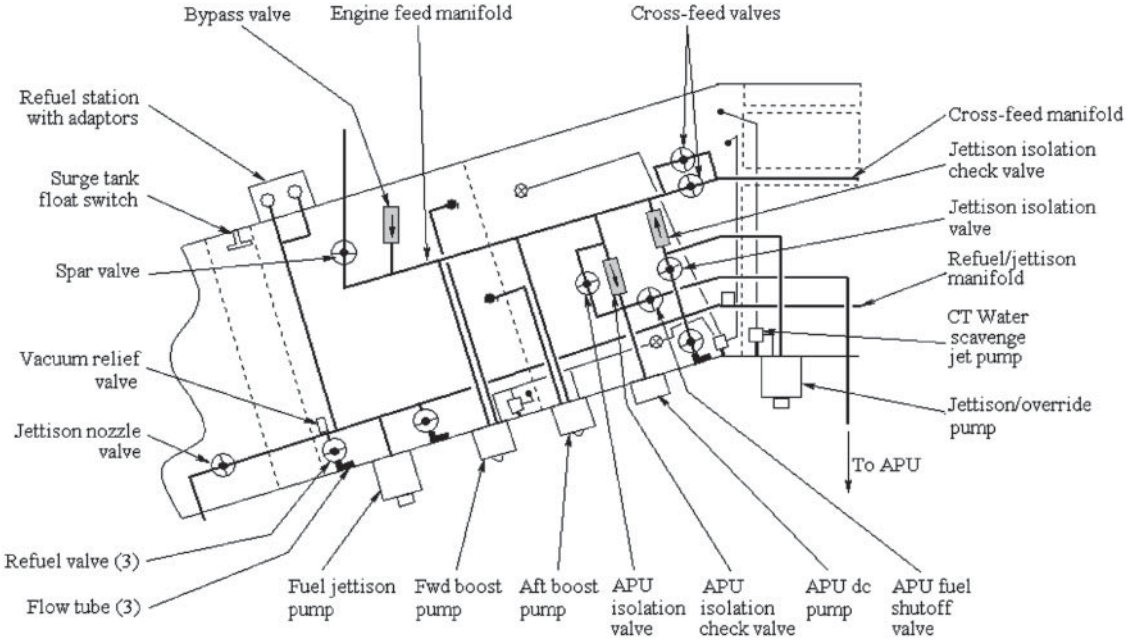

Fig. 1 Boeing 777-200 fuel system (left side)

Table 1 Engine feed phase monitoring variables

	Engine feed phase									
	1 (CT feed)		2 (MT feed)		3 (cross-feed L–R)		4 (cross-feed R–L)		5 (MT suction feed)	
Variable	Left	Right	Left	Right	Left	Right	Left	Right	Left	Right
CT level	>0	>0	$\leqslant$L2 and >0	$\leqslant$L2 and >0	—	—	—	—	—	—
MT level	LSV	LSV	>0	>0	>0	>0	>0	>0	$\geqslant$L2	$\geqslant$L2
Jettison/override pump switch	On	On	Off	Off	Off	Off	Off	Off	Off	Off
Jettison/override pump pressure light	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off
Aft boost pump switch	Off	Off	On	On	On	Off	Off	On	Off	Off
Aft boost pump pressure light	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off
Forward boost pump switch	Off	Off	On	On	On	Off	Off	On	Off	Off
Forward boost pump pressure light	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off
Engine flow meter	FW	FW	FW	FW	FW	FW	FW	FW	FW	FW
Spar valve switch (fuel control switch)	Run	Run	Run	Run	Run	Run	Run	Run	Run	Run
Spar valve and spar relay position	AGR	AGR	AGR	AGR	AGR	AGR	AGR	AGR	AGR	AGR
Cross-feed valve 1 (CFV1) switch	Off	—	Off	—	On	—	On	—	Off	—
Cross-feed valve 1 and switch position light	Off	—	Off	—	Off	—	Off	—	Off	—
Cross-feed valve 2 (CFV2) switch	Off	—	Off	—	On if CFV1C		On if CFV1C		Off	—
Cross-feed valve 2 and switch position light	Off	—	Off	—	Off	—	Off	—	Off	—

CT, centre tank; MT, main tank; L2, level 2; FW, flow; AGR, agree; CFV1C, cross-feed valve 1 closed; LSV, load select value.

using the integrated refuel panel on the left wing where either manual or automatic refuel is selected. In the case of manual refuel, the operator controls the flow of fuel into the tanks by opening and closing the refuel valves. During automatic refuel, the required tank levels are set by the operator, and control loops determine when the system should remove power from the refuel valves, thus resulting in their closure.

The pressure refuel operating mode is divided into two main phases and a single override phase. In order to determine the behaviour of the system, tank level readings and fault indicating methods, such as valve lights and control switch positions, are used (shown in Table 2, under column headed 'Variable').

Phase one. Fuel is pumped from the refuelling source into the main and centre tanks via the refuel manifold. While the tank levels are below their load select value (LSV, the amount of fuel required as selected by the operator) the refuel valves are expected to be open with their respective refuel lights on. When conducting manual refuel the operator is required to turn the refuel valve control switches into the 'Open' position. The control switches are not utilized in the automatic mode.

Phase two. Once the main and centre tanks reach their respective LSVs the refuel valves are closed, either by the operator during manual refuel or automatically via the level control loop.

Override phase. Should fuel flow from either main tank into their associated surge tanks and activate the surge tank reed switches, a signal is transmitted to remove power from all of the refuel valves. This results in their closure and the non-transferral of fuel from the refuel manifold to the main and centre tanks.

2.3 Component failure modes

The component failure modes considered in the analysis are shown in Table 3. It is assumed that the stated failure modes may affect the functionality of the aircraft fuel system. Each component failure mode is allocated a code associated to a related component identification tag.

Table 2 Pressure refuel mode monitoring variables

	Pressure refuel phase					
	Manual			Automatic		
Variable	Phase 1	Phase 2	Override	Phase 1	Phase 2	Override
CT level	< LSV	LSV	LSV	< LSV	LSV	LSV
Left MT level (LMTL)	< LSV	LSV	LSV, >LSV if RMTL = LSV	< LSV	LSV	LSV, > LSV if RMTL = LSV
Right MT level (RMTL)	< LSV	LSV	LSV, >LSV if LMTL = LSV	< LSV	LSV	LSV, > LSV if LMTL = LSV
CT refuel valve control switch	Open	Closed	—	—	—	—
Left MT refuel valve control switch	Open	Closed	—	—	—	—
Right MT refuel valve control switch	Open	Closed	—	—	—	—
Left CT refuel valve light	On	Off	Off	On	Off	Off
Right CT refuel valve light	On	Off	Off	On	Off	Off
Left MT outboard refuel valve light	On	Off	Off	On	Off	Off
Left MT inboard refuel valve light	On	Off	Off	On	Off	Off
Right MT outboard refuel valve light	On	Off	Off	On	Off	Off
Right MT inboard refuel valve light	On	Off	Off	On	Off	Off

LSV, load select value; RMTL, right main tank level; LMTL, left main tank level.

Table 3 Component failure modes

Operating mode	Component	Failure mode
Engine feed and refuel	Manifold	Blocked, partially blocked, fractured
Engine feed	Tank (centre and main)	Fractured
Engine feed and refuel	Pipe, flow tube	Blocked, partially blocked, fractured
Engine feed	Jettison isolation check valve	Failed closed
Engine feed	Pump	Run, no run
Engine feed and refuel	Spare valve, outlet float operated valve, inlet float operated valve, outboard refuel valve, inboard refuel valve, refuel valve, drain valve, vacuum relief valve	Failed open, failed closed, failed in intermediate position
Engine feed	Cross-feed valve	Failed open, failed closed
Refuel	Refuel valve switch, refuel valve position switch	Open (faulty), closed (faulty)
Refuel	Surge tank float switch, tank unit	Failed high, failed low

3 THE DIGRAPH METHOD

3.1 Digraph description

A digraph is constructed from a set of nodes and edges [**15**]. The nodes represent system process variables and the edges connecting the nodes illustrate the interrelationships that exist between components in a system. Nodes are also used to represent component failure modes, whereby a signed edge connecting a failure mode node to a process variable node indicates the resulting disturbance caused by the failure mode.

Digraph nodes contain an alphanumeric label which symbolizes a specific process variable or component failure mode. With regards to process variable nodes, the precursor to the numeric section indicates the type of process variable the node represents, i.e. an M may be used to represent mass flow. The numeric section of the label corresponds to a precise location in the application system, i.e. M102 could represent the mass flow at location 102. Process variable deviations are expressed as one of five discrete values, +10, +1, 0, −1, and −10, corresponding to large high, small high, normal, small low, and large low deviations [**16**, **17**].

A simple digraph is illustrated in Fig. 2. It can be noted that M1 and M2, the nodes, are connected by two edges. The alphanumeric code M1 represents mass flow at location 1. The edge with a gain of +1 is considered to be the normal edge since this represents the relationship that is normally true; mass flow at location 1 has a positive effect on mass flow at location 2 (M2). The second edge in the illustration is termed a conditional edge because its relationship is only true whenever the condition represented by ':' exists. It must be noted that only one edge is true at any one time.

The standard method of constructing a digraph for a system is followed in this research. It is from this model that the diagnostic procedure has been developed: it stems from the initial determination of deviations from normal system operation. 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 conducted by marking all of the nodes affected by the initial highlighting. This process, termed 'back-tracing', is described further in section 3.2.

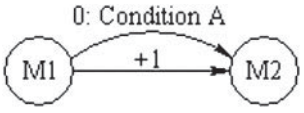

Fig. 2 A simple digraph

3.2 Diagnostic procedure

The procedure for diagnosis can be broken down into three phases. The first involves the model construction, the second the diagnosis itself, with the third for honing in on the actual fault cause. A generalized procedure outlining the main steps involved in developing a system digraph (phase 1) is provided.

1. *System analysis*. Firstly the system under investigation is defined. A specific number is allocated to each component so generating a straightforward location reference approach for process variables and component failure modes at a given point. All relevant component failures of the system are compiled. A failure mode code is then attached to each fault. The system is also separated into subunits and components.
2. *Digraph generation*. The unit digraph models for the subunits, previously noted in step 1, are generated. All process variable deviations that could have an effect on the variables in the model are taken into consideration. The extent of the effect any disturbance may have on the system with regards to the assigning of discrete values is also noted. The system digraph is formed by connecting common variables from the subunit models.

The fault diagnostics process is conducted using the system digraph (phase 2). System behaviour can be monitored using data retrieved from sensors. In a given mode of operation the system would have a set of expected sensor readings. These are compared with the actual system readings during the diagnostics procedure (steps 3 to 5) to identify the presence of any deviations.

3. *Determination of system deviations*. The expected system sensor readings are noted. The actual sensor readings from the system are retrieved and then compared with those expected to determine the existence of any deviations.
4. *Flagging of non-deviations*. Non-deviating sensor nodes in the digraph are 'flagged'. It is assumed that a non-deviating reading indicates the absence of a failure.
5. *Back-tracing process*. If a sensor registers a deviation then fault diagnosis involves back-tracing through the system digraph from the node that represents the location of the given deviation. The back-tracing process ceases once either (a) a flagged section is reached or (b) no more back-tracing is possible. For multiple deviating sensors the diagnostic results obtained through back-tracing from each deviating node are ANDed together. All potential fault causes are listed at the end of the fault diagnostics procedure.

Following the back-tracing process, often a list of potential causes is produced; therefore the final stage (phase 3) of the diagnostic procedure is to hone in on the most probable fault cause. Three steps are advised.

6. *Identification of faulty component*. Reduction of the fault list is carried out by removing component failure modes to identify solely the component(s).
7. *Specificity of component fault*. Numerical rankings are calculated using importance measures to identify the most likely contributor to the system deviation.
8. *Evidence of fault*. Data from maintenance logs can be used to modify rankings to further hone in on the problem source.

4 CASE STUDY – APPLICATION OF DIAGNOSTICS APPROACH

4.1 Phase 1 – fuel system digraph development

With the system defined and component failure modes identified, the next step involves generating the system digraph. A digraph is generated for each operating mode. For the engine feed the fuel system is split into three main sections: (a) cross-feed, left centre, and main tank; (b) right centre; and (c) main tank. In total, the system digraph for the engine feed phase is constructed from 282 nodes, of which 88 are process variable nodes and 194 are component failure mode nodes. The unit digraphs for the centre and main tanks (left and right wings) are developed through a process of building up from the tank levels nodes to the fuel pumps, engine feed manifold, and spar valves at the inlet to the engines. The cross-feed section digraph encompasses the pipe-work and related valves that connect the left and right engine feed manifolds.

With regards to the pressure refuel operating mode, the system is divided into three groups: left wing section, right wing section, and the third group – the associated control loops and signal structure (control loops are dealt with in a separate group owing to both their importance within the pressure refuel operating mode and the fact that there are numerous integrated loop and signal structures present). In total the fuel system digraph associated with the pressure refuel operating mode is constructed from 228 nodes, of which 50 are process variable nodes and 178 are component failure mode nodes.

A section of the respective left main tank digraph for the engine feed mode is presented in Fig. 3. This depicts the relationship exhibited in a section of the pipe-work incorporating a spar valve and suction bypass valve in the left wing. Mass flow along the left engine feed manifold is represented by the process

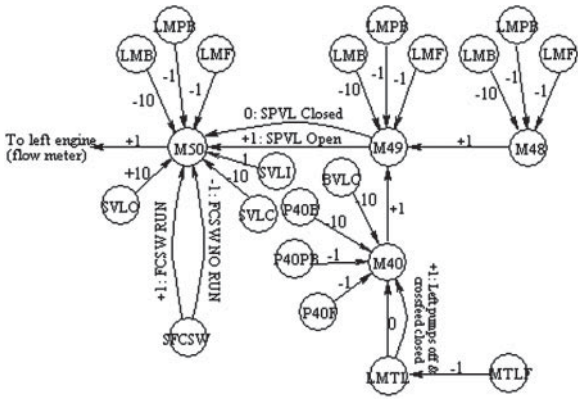

Fig. 3 Left main tank digraph section for engine feed mode

flow structure exhibited by nodes M48 → M50. The direction of flow in the manifold, and hence the direction of the edges connecting the mass flow nodes, is towards the spar valve which allows fuel to pass to the left engine. There are three identical failure modes associated with the mass flow nodes that represent the left engine feed manifold. Two failure modes, left engine feed manifold fractured and partially blocked (LMF, LMPB), result in a small negative disturbance, and the left engine feed manifold blocked (LMB) mode results in a large negative disturbance. These disturbances are indicated by signing the edges, connecting the failure mode nodes to the process variable nodes, '−1' and '−10'.

The left spar valve is denoted by the relationship between nodes M49 and M50. If the spar valve is closed then this normally positive relationship is nullified, as indicated by the conditional edge signing '0: SPVL Closed'. There are three spar valve failure modes that may result in a disturbance on mass flow entering the left engine: spar valve open (SVLO), spar valve closed (SVLC), and spar valve intermediate position (SVLI). The failure modes would generate a large positive, large negative, and small negative disturbance respectively. These deviations are indicated by the signs '+10', '−10' and '−1' on the edges connecting the failure mode nodes to M50. The node SFCSW, fuel control switch node, and M50 illustrate the control relationships from the pilot inputs for the spar valve. If the switch is set to 'run' then the relationship is positive (+1: FCSW RUN), else a negative relationship is exhibited (−1: FCSW NO RUN). A more detailed explanation of the digraph section is explained in reference [**14**].

4.2 Phase 2 – performing diagnostics

4.2.1 Observed and expected system behaviour

The method for performing system diagnostics using digraphs is based on comparing system sensor readings with those that would be expected while the

system is in a known operating mode. The first step therefore involves determining if any system variable deviations exist. The presence of a deviation is considered indicative of a fault having occurred. It is assumed that a non-deviating transmitter reading indicates the absence of failure in its respective section. Tables 1 and 2 show the expected readings for the sensors in the system for each given mode of operation.

4.2.2 *Diagnostic considerations*

A general diagnostic statement, which is applicable to both the engine feed and pressure refuel modes, regards the relationship between a switch and its associated controlled device. Both the deviations and non-deviations noted by the switch and sensors that are located near the device are used to 'hone in' on specific fault options. Further information is provided in reference [**14**].

All control aspects of the engine feed mode are instigated through pilot–switch interfaces. The pilot makes informed decisions based on the data retrieved from the flow meters and tank levels, as well as the indication lights. Consequently, when back-tracing along the routes between the switches and controlled components, there is no need to consider the paths separately. Loop operators [**17**] need not be employed since they do not form 'complete' control loops. This is not, however, the situation during the pressure refuel operating mode since upstream variables are used by the system to regulate downstream variables without the involvement of a human operator.

The control aspects associated with the pressure refuel operating mode are subdivided into three segments, one of which is completely manual and instigated through an operator–switch interface while the remaining two are automatic. During the manual operation of the pressure refuel mode, the operator conducts informed decisions based on retrieved tank level data. As a result, when back-tracing along the routes between the valve control switches and the controlled components there is no need to consider the paths separately. Conversely, during automatic operation of the refuel mode a downstream variable, the tank level, is used by the system to regulate the refuel valves (upstream variables). Therefore, while back-tracing through the negative feedback loop, the loop must be considered as an entire entity. The third 'control loop' is related to the override function of the surge tank level switches and consequently forms an override control route as opposed to a loop. Therefore, depending on the precise phase of the pressure refuel operating mode, sections of the digraphs are 'turned on and off' accordingly. For example, should the system be running in manual with all tank levels below their LSVs and no noted refuel valve deviations, the override and automatic refuel mode control sections are disregarded.

4.2.3 *Back-tracing*

Where no deviation exists between the expected and actual system behaviour the corresponding nodes in the digraph, representing the relevant process variables, are 'flagged'. Back-tracing commences from the location of any noted deviations to determine the possible fault causes. The process of back-tracing ceases once a flagged node is reached or if no further back-tracing can take place. A single faulty fuel system scenario is used to illustrate the diagnostic capability of the fuel system digraph. The system is assumed to be in phase 5 of the engine feed operating mode. The retrieved readings note a single deviation from those expected (highlighted in bold in the subset of sensor readings shown in Table 4); 'no flow' is registered by the left flow meter instead of 'flow'. The readings are retrieved at 30 s intervals.

The process of back-tracing is automated through running scripted code in Matlab. The diagnostic program can be subdivided into four main sections, namely: input, comparison, fault diagnostics, and output. These are discussed in detail in reference [**14**]. The diagnostic results are displayed while the program runs. Initial display features involve noting the status of the fuel system sections with regards to the presence or absence of any noted deviations. If deviations are noted, the determined fault diagnostic results are displayed on screen for each section. When reading the retrieved actual data into the program, results are output for each interval. For the first three intervals it is noted that no deviations exist. A deviation is recorded in the left wing during interval four ($t = 90$ s).

Table 4 Expected and retrieved readings

	Expected		Retrieved (after 90 s)	
Variable	Left	Right	Left	Right
Forward boost pump switch	Off	Off	Off	Off
Forward pressure light	Off	Off	Off	Off
Engine flow meter	Flow	Flow	**No flow**	Flow
Spare valve switch	Run	Run	Run	Run

1. During the fault diagnostics process for interval four, the right wing and cross-feed section flags are signed '0' while the left wing flag is signed '1', thus indicating the presence of a transmitter deviation. Variable deviations are represented using five discrete values [+10, +1, 0, −1, −10] (noted in section 3.1). Taking into account the example described in section 4.2.1, the deviation 'no flow' is registered as opposed to the expected variable 'flow'. Full flow and no flow are considered to be the maximal registered readings. Therefore, the deviation 'no flow' in the example is accounted for using '−10' → large negative deviation, where '10' represents the magnitude. Back-tracing commences from node M50(−10) and, given the stated operating mode phase, considers the process flow structure in the digraph that represents the left engine feed manifold and suction bypass valve. Node M50 marks the location of the transmitter deviation at the inlet to the left engine and '−10' takes into account the magnitude of the registered deviation. The back-tracing procedure ceases at the main tank level node. The fault propagation can be followed by referencing Fig. 4:

    1. M50 (−10) → LMB.
    2. M50 (−10) → M49 (−10) → M40(−10) → P40B, BVLC.

The failure mode LMB is omitted in the fault propagation M50 → M49 since it has already been determined from point 1 above. The back-tracing sequence is thus simplified, as the full results list 'LMB + LMB + P40B + BVLC' would be reduced to 'LMB + P40B + BVLC'. This simplification process is automated within the diagnostic program.

Three diagnostic results are output by the program: left engine feed manifold blocked (LMB), pipe 40 blocked (P40B), and left suction bypass valve closed (BVLC). A fourth failure mode (SVLC) illustrated as causing a large negative disturbance on flow at location 50 (M50) in Fig. 4 is not listed. The spar valve is not considered to have failed closed given that the spar switch is in the 'Run' position and no warnings have been issued to the pilot regarding a disagreement between the spar valve and spar valve switch positions. The final phase of diagnosis is discussed in section 5.

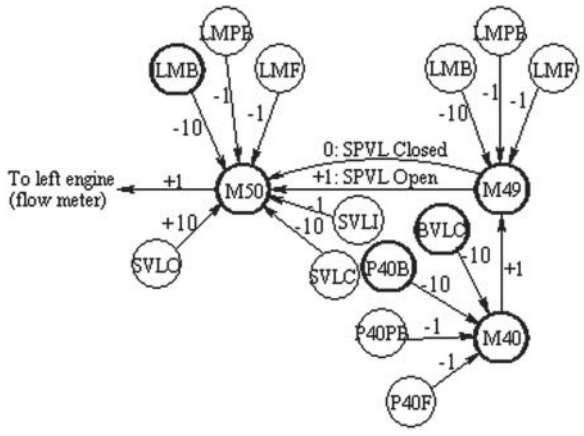

Fig. 4 Back-tracing illustration

4.3 Results

In order to test the diagnostic strategy, results for single and multiple deviating transmitter readings have been obtained for other example scenarios covering the entire range of the engine feed and pressure refuel operating modes. Ten test cases are summarized in Table 5. The actual readings and the number of failure modes determined are highlighted. The 'number of faults determined' refers to the number of faults obtained through the back-tracing procedure for the specified test case. 'First order' indicates one fault, 'second order' two faults (multiple failure), etc. It can be observed that often more than one fault cause is identified. It should be noted that the actual fault causes for the noted test cases are obtained in these examples. The key issue highlighted is how to improve the distinguishability of the diagnostic strategy. Two methods are discussed in section 5. The addition of further transmitters into the system would allow for increased isolability. A compromise has to be found, though, between the over-complexity issues involved in the addition of further sensors and the precise identification of failures.

When dealing with sensor readings to identify the system behaviour the technique must be able to overcome the issue of sensitivity. Thresholds for the level, flow, and pressure readings are determined so as to prevent 'false alarms' with regards to registered deviations. In this application this has been sufficient to produce valid results; however, a more advanced technique may need to be investigated for differing applications.

Caution must be exercised to ensure that the model created of the system actually reflects the physical system. With detailed piping and instrumentation illustrations, and using expert knowledge, verification of the expected relationships has been sought. While working with an actual system a period of testing would need to be carried out to verify the models created.

On dealing chiefly with mass flow relationships in the fuel system the diagnostic back-tracing procedure is sufficient since transmitter readings are taken downstream of prospective failure locations. It may, however, be necessary to consider 'forward-tracing'

Table 5 Ten test case results

Test case	Operating mode	Registered deviations	No. of faults determined
1	Engine feed	*Left main tank* Flow meter: no flow	2: 1 first order 1 second order
2	Engine feed	*Left main tank* Forward boost pump pressure light: on Aft boost pump pressure light: on Flow meter: no flow	36: 4 first order 16 second order 16 third order
3	Engine feed	*Left centre tank* Level transmitter: static level	6: 3 first order 3 second order
4	Engine feed	*Left main tank* Cross-feed valve 1 switch position light: on	1: 1 first order
5	Engine feed	*Right main tank* Forward boost pump pressure light: on Aft boost pump pressure light: on Flow meter: reduced flow *Left main tank* Flow meter: reduced flow	28: 4 first order 8 second order 16 third order
6	Pressure refuel	*Left main tank* Level transmitter: static level Inboard refuel light: off Outboard refuel light: off	4: 4 second order
7	Pressure refuel	*Right centre tank* Refuel light: off	2: 2 first order
8	Pressure refuel	*Centre tank* Level transmitter: low rate of level increase *Left main tank* Level transmitter: static level	4: 3 first order 1 second order
9	Pressure refuel	*Centre tank* Level transmitter: static level *Right main tank* Level transmitter: static level Inboard refuel light: off Outboard refuel light: off *Left main tank* Level transmitter: static level Inboard refuel light: off Outboard refuel light: off	1: 1 second order
10	Pressure refuel	*Centre tank* Level transmitter: static level *Right main tank* Level transmitter: static level *Left main tank* Level transmitter: static level	16: 9 second order 6 third order 1 fourth order

when reviewing applications with numerous complex relationships which span across subsystems.

With the inclusion of the second operating mode of refuel the method ultimately illustrates the potential for application to an actual aircraft fuel system comprising a built-in control loop structure, thus addressing some of the issues surrounding scalability of the method. By breaking the operating mode into separate sections this has prevented the generation of unwieldy models.

5 LOCATION AND SPECIFICITY OF FAULT

Current diagnostic results produced from the program often include a multitude of possible causes. Research has focused on three ways to reduce this list and identify the most likely cause, if not actual cause, of the system deviation (phase 3 of the diagnostic process). The first method (section 5.1) considers an approach to identify the component at fault, to direct maintenance engineers to the source of the problem. The second (section 5.2) looks at using mathematical techniques combined with component failure and repair statistics to highlight the most likely component failure mode combination. The final method involves reviewing current maintenance logs to adjust the rankings in accordance with the supporting evidence on the possible problem source.

5.1 Determining the component at fault

The first method is based on the principle of retrieving the diagnostic results from the full analysis, and then reducing the list through removing the component failure modes and simply listing the components

that may be faulty. It is assumed that the operator conducting the diagnostic analysis is primarily interested in the actual component that is known to be faulty. For example, if pipe X is noted as either leaking or ruptured, it is pipe X that is of significance as opposed to the definitive failure mode. Inspection of this identified component will then yield the actual failure mode. The reduction procedure is applied to a test case as a means of exemplifying the proposed process.

5.1.1 Engine feed test case

The diagnostic results retrieved from application of the digraph approach yield 4 second-order fault combinations and 16 combinations of both the orders three and four. Through considering the removal of specific failure modes and simply listing the relevant components, the fault list is cut to 12 multiple faults, 4 of the orders two, three, and four. The revised list is thus presented

(Order 1) ABL.FBL, ABL.P59, FBL.P58, P58.P59
(Order 2) LM.ABL.FBL LM.ABL.P59, LM.FBL.P58, LM.P58.P59
(Order 3) ABL.FBL.P55.P56, ABL.P59.P55.P56, FBL.P58.P55.P56, P55.P56.P58.P59

where: LM is left manifold; ABL is left aft boost pump; FBL is left forward boost pump; P55, P56, P58, and P59 are pipes 55, 56, 58, and 59.

From the test case it is noted that, depending on the precise component failure modes retrieved for the scenario under investigation, the reduction process can have a noticeable effect. However, on some occasions the number of fault combinations listed is not reduced. This is due to the fact that the failure modes retrieved from the initial analysis are all associated with separate components. For scenarios where the reduction process is applicable, it is effective in reducing the diagnostic list previously yielded.

5.2 Determining the most probable failure mode cause

A method that has been developed to identify the most probable failure mode cause is to use reliability theory [**18**]. Unavailability functions and importance measures are utilized in order to rank the failure combinations yielded accordingly. It is assumed that the repair process would be initiated once a failure is revealed and therefore the unavailability is given by

$$Q(t) = \frac{\lambda}{\lambda + \nu}(1 - \mathrm{e}^{-(\lambda+\nu)t}) \tag{1}$$

where λ is failure rate, ν is repair rate, and t is time. Generic failure rate data [**19**] are employed in equation (1) as a means of defining the fuel system component's unavailability. For the example given in section 4.2.3, the unavailability of the relevant components was found to be: LMB, 1.69×10^{-7}; BVLC, 5×10^{-8}; P40B, 3×10^{-10}. The Fusell–Vesely measure of minimal cut set importance provides a means of ranking the cut sets obtained from the system digraph. The expression for the Fusell–Vesely measure is illustrated by

$$I_i = \frac{P(C_i)}{Q_{\mathrm{SYS}}(q(t))} \tag{2}$$

The importance measure is defined as the probability of occurrence of cut set i $[P(C_i)]$ given that the system has failed. Q_{SYS} is calculated using the rare event approximation as opposed to calculating an exact value. For the given example, no difference was noted in the ranking of the cut sets when considering either the rare event or exact values for Q_{SYS}. For cases whereby many cut sets are produced, it would be computationally demanding to determine an exact value for Q_{SYS}.

For the example, the cut set importance measures were found to be ($Q_{\mathrm{SYS}} = 2.20\times10^{-7}$): LMB, 7.71×10^{-1}; BVLC, 2.28×10^{-1}; P40B, 1.37×10^{-3}. From the results the most likely cause for the given deviation at the inlet to the left engine flow meter is noted as a blockage in the left engine feed manifold. In addition, this method of ranking can be combined with the reduced list of failed components developed in section 5.1.

5.3 Evidence of component fault

Each aircraft has a complete technical log, which consists of three volumes: an aircraft technical log; a cabin discrepancy log; and an in-flight entertainment defect log. This technical log reflects the current status of defects, repairs, replacements, adjustments, and inspections while the aircraft is in service. The entries placed in the log form a permanent part of the aircraft records. The extension to the honing-in method proposed considers information contained in the aircraft technical log. The approach is applicable once the initial analysis, based on reliability theory, has been conducted. Throughout the analysis it is assumed that the aircraft holds a valid Certificate of Airworthiness and all relevant maintenance checks have been conducted before departure. The proposed extension procedure to be followed is:

(a) the 'defect' section of the Sector Record is referenced;
(b) the list of defect descriptions is cross-referenced with the ranked failure combinations; any failure combinations that are not associated with the noted defects are initially masked;

(c) the action taken by maintenance personnel is then researched; from the noted defects in the technical log it is possible to re-rank the cut sets accordingly;
(d) for scenarios involving fault combinations that are not associated with the entered defects, technical engineering knowledge of the system must be used to locate the actual system fault within the ranked results list, previously obtained using reliability theory.

The extension method is based upon the presumption that 'Nil defects' is not entered in the defect section of the Sector Record. In order to illustrate how the maintenance log information may be used, consider the example where upon implementation of the previous honing-in mechanism the failures are ranked in the order:

(a) LMB (left manifold blocked);
(b) P56B.P55B (pipes at locations 56 and 55 blocked).

From the aircraft technical log it is noted that: (a) the aircraft recently underwent a scheduled maintenance review during which the left spar valve in the engine feed manifold was replaced along with partial manifold resealing work; (b) there are no deferred fuel system defects listed; (c) daily and pre-departure checks revealed no fuel system defects.

Since the noted fuel system repair work was conducted on components associated with the engine feed manifold, the most probable fault cause is deemed to be a blockage in the left manifold. It is likely that a foreign object, left by maintenance after undertaking repairs, resulted in the blockage. In this case both the initial honing-in mechanism and the extension using logs list 'LMB' as the most probable fault cause. Here the technical log has provided supporting evidence; for other instances it may reweight component failure modes as more or less probable. Incorporation of this information to form a fully automated procedure would be of further benefit.

6 CONCLUSION

The fuel system digraph noticeably reflects the physical structure of the system under investigation, thus providing a clear representation of the relationships that exist between the system variables. The complete digraph for the fuel system is relatively large in terms of the number of nodes from which the digraph is constructed. The development process is, however, greatly aided by dividing the system into subunits and operating modes.

The potential for the presence of anomalies between failure mode results is eradicated through incorporating 'flagging' into the diagnostics process. 'Flagging' is considered a consistency check and therefore removes the possibility of conflicting results arising between non-deviating transmitter nodes and the failure results achieved through back-tracing from nodes noting specific deviations. This process has been adapted further when considering the five defined phases of the engine feed operating mode, in addition to the alternative operating mode of refuel. Depending on the specific phase and mode of operation, sections of the system digraph are effectively turned 'on' or 'off' accordingly. This therefore dictates the route to be followed when back-tracing from a deviating node.

The use of reduction in failure combination lists helps to hone in on the specific component at fault, and the use of reliability theory permits the presentation of a numerical solution to determine the most likely fault cause for a given deviation. In this manner it is possible to provide a complete list of the fault causes yielded through back-tracing, while also highlighting the location of the fault, i.e. the problem component, and also indicating the actual fault that is considered to have occurred. The use of maintenance logs further helps to provide evidence of the exact cause of the fault. This development builds on previous research where a honing-in mechanism was cited as necessary when considering faulty scenarios that yield numerous diagnostic results. Ultimately examination of the system may be required to determine the exact fault cause in some instances.

Current research considers a range of phases and operating modes and deals with multiple faults. Furthermore, real-time diagnosis is allowed for through computer analysis. Control loop operators have been employed during the fault diagnostics process when taking into account the control loop associated with the refuel mode, thus demonstrating the feasibility of this technique as a fault diagnostic method.

REFERENCES

1 **Papadopoulos, Y.** and **McDermid, J.** Automated safety monitoring: a review and classification of methods. *Int J. Condition Monitoring Diagnostic Engng Managmt*, 2001, **4**(4), 1.
2 **Novak, F., Žuzek, A.,** and **Biasizzo, A.** Sequential diagnosis tool. *Microproc. Microsyst.*, 2000, **24**(4), 191.
3 **Pattipati, K. R.** and **Alexandridis, M. G.** Application of heuristic search and information theory to sequential fault diagnosis. *IEEE Trans. Syst., Man Cybern.*, 1990, **20**(4), 872.
4 **Shakeri, M., Raghavan, V., Pattipati, K. R.,** and **Patterson-Hine, A.** Sequential testing algorithms for multiple fault diagnosis. *IEEE Trans. Syst. Man Cybern. – Part A: Syst. Humans*, 2000, **30**(1), 1.

5 **Price, C.** AutoSteve: electrical design analysis. *Coll. Dig. – IEE*, 1997, **338**(4).

6 **Price, C.** and **Taylor, N.** Multiple fault diagnosis from FMEA. In Proceedings of the National Conference on *Artificial Intelligence*, Providence, Rhode Island, 1997, p. 1052.

7 **Hurdle, E., Bartlett, L.,** and **Andrews, J.** System fault diagnostics using fault tree analysis. In Proceedings of the 16th Advances in Reliability Technology Symposium, Loughborough, 2005, p. 203 (Loughborough University).

8 **Papadopoulos, Y., Parker, D.,** and **Grante, C.** Automating the failure modes and effects analysis of safety critical systems. In Proceedings of the 8th IEEE Symposium on *High Assurance Systems Engineering*, Tampa, USA, March 2004, p. 310.

9 **Vedam, H.** and **Venkatasubramanian, V.** Signed digraph based multiple fault diagnosis. *Comput. Chem. Engng (Suppl.)*, 1997, **21**, S655.

10 **Palmer, C.** and **Chung, P.** Creating signed directed graph models for process plants. *Ind. Engng Chem. Res.*, 2000, **39**(7), 2548.

11 **Maurya, M., Rengaswamy, R.,** and **Venkatasubramanian, V.** A systematic framework for the development and analysis of signed digraphs for chemical processes. 1. Algorithms and analysis. *Ind. Chem. Engng Res.*, 2003, **42**(20), 4789.

12 **Venkatasubramanian, V., Rengaswamy, R., Yin, K.,** and **Kavuri, S.** A review of process fault detection and diagnosis. Part I: quantitative model-based methods. *Comput. Chem. Engng*, 2003, **27**(3), 293.

13 **Price, C.** *Computer-based diagnostic systems*, 1999 (Springer-Verlag, London).

14 **Kelly, E.** and **Bartlett, L.** Improved fault diagnostics for a dynamic aircraft fuel system using the digraph approach. In Proceedings of the European Safety and Reliability Conference, *Risk, Reliability and Societal Safety*, 2007.

15 **Kohda, T.** and **Henley, E.** On digraphs, fault trees and cut sets. *Reliab. Engng Syst. Saf.*, 1998, **20**(1), 35.

16 **Andrews, J.** and **Morgan, J.** Application of the digraph method of fault tree construction to process plant. *Reliab. Engng*, 1986, **14**(2), 85.

17 **Andrews, J.** and **Brennan, G.** Application of the digraph method of fault tree construction to a complex control configuration. *Reliab. Engng Syst. Saf.*, 1990, **28**(3), 357.

18 **Andrews, J.** and **Moss, T.** *Reliability and risk assessment*, 2002 (Professional Engineering Publishing, London).

19 **Moss, T.** *The reliability data handbook*, 2005 (Professional Engineering Publishing, London).