Aircraft fuel rig system fault diagnostics based on the application of digraphs

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

The manuscript was received on 3 May 2007 and was accepted after revision for publication on 25 July 2007.

DOI: 10.1243/1748006XJRR88

Abstract: The issue of fault diagnostics is a dominant factor concerning current engineering systems. Information regarding possible failures is required in order to minimize disruption caused to functionality. A method proposed in this paper utilizes digraphs to model the information flow within an application system. Digraphs are composed from a set of nodes representing system process variables or component failure modes. The nodes are connected by signed edges thus illustrating the influence, be it positive or negative, one node has on another. System fault diagnostics is conducted through a procedure of back-tracing in the digraph from a known deviating variable. A computational method has been developed to conduct this process. Comparisons are made between retrieved transmitter readings and those expected while the system is in a known operating mode. Any noted deviations are assumed to indicate the presence of a failure. The current paper looks in detail at the application of the digraph diagnostic method to an industrially based test stand of an aircraft fuel system. This research includes transient system effects; the rate of change of a parameter is taken into consideration as a means of monitoring the system dynamically. The validity of the results achieved, through performing fault diagnostics based on the use of a digraph model, is evaluated. Finally, the effectiveness and scalability issues associated with the application of the method are addressed.

Keywords: system fault diagnostics, digraphs, aircraft fuel system

1 INTRODUCTION

With the growing intolerance towards failures within systems fault diagnosis has become a fundamental facet of engineering applications. It is concerned with isolating the underlying causal faults leading to an observable effect in a monitored process. Effective detection of system faults aids in decreasing downtime and thus improves operational stability [**1**]. Methods employed to identify faults can be classified according to model-based, case-based, and rule-based strategies. The emphasis of the research presented in this paper lies within model-based diagnosis (MBD), where models of a system are used as the basis for performing fault diagnostics. MBD is particularly suited to systems whose architecture comprises either the same or similar components.

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

Novak *et al.* [**2**] focus on generating a sequential diagnosis tool (SDT). The SDT highlights a prospective fault through running a series of tests at a particular point in time. This rule-based approach has been proven to be effective when determining single faults in a system with a known period of inactivity. However, difficulties arise when considering the complexity issue surrounding dependency in multiple fault combinations. Shakeri *et al.* [**3**] successfully extend the sequential testing technique through attempting to determine multiple fault causes for a given test. From the results, further research is required to consider both unreliable tests and the combining of diagnostic results to form multiple failure options in fault tolerant systems (systems displaying redundancy).

Failure modes and effects analysis (FMEA) is an established system safety analysis technique. Attempts have been made to automate the process and thus increase its effectiveness through decreasing the time required to perform the analysis [**4**, **5**]. Limitations

have involved difficulties with the efficiency and scalability of the algorithms utilized. A different approach, proposed by Papadopoulos *et al.* [**6**], considers translating the information contained within a network of interconnected fault trees into FMEA-style tables. Variability, with regard to performance, is exhibited with increased system complexity.

Digraphs, also known as signed directed graphs [**7**, **8**], can illustrate specific fault propagations through a system. The issues involved with diagnosing single faults in systems are addressed by Rao [**9**]. Iverson and Pattersine-Hine [**10**] extend this approach by considering the combination of two failures via an AND gate, and identify the potential for real-time automated monitoring and diagnosis.

The characteristics associated with modern-day systems require fault diagnostic strategies to incorporate both adaptability and the identification of multiple faults [**11**]. Modern systems are of varying size and complexity and are thus usually required to operate in more than one mode. It is therefore considered beneficial for an ideal diagnostic procedure to incorporate an adaptable scope.

The present paper applies the digraph method to a simulation test stand which is representative of an aircraft fuel system (section 4). The purpose of an aircraft fuel system is reliably to provide the required amount of fuel to the engines during all phases of flight. A fuel system is thus integral to an aircraft set-up. The main issues affecting the fault diagnostics of an aircraft fuel system on a macro scale cover fuel storage, distribution, dump, and variable transmitters (e.g. level transmitter). The analysis conducted addresses fuel storage and distribution through taking three operating modes into account. Fuel dump is considered during the drain phase. For the purposes of this research it is assumed that the variable transmitters provide reliable readings.

The issues surrounding multiple faults and dynamic analysis are also addressed. A brief insight into digraphs through considering their representation of fault propagations in a system is provided in sections 2 and 3. System fault diagnostics taking into account transient effects and the results yielded through automating the procedure are reviewed in sections 4 and 5. The conclusions of the research are presented in section 6.

2 THE DIGRAPH METHOD

A digraph [**12**] is constructed from a set of nodes and edges, which are used to illustrate the 'cause–effect' relationships present within a system [**13**–**15**]. The nodes represent system process variables or component failure modes, and the edges connecting the nodes illustrate the interrelationships that exist between components in a system. Digraph nodes contain an alphanumeric label which symbolizes a specific process variable or component failure mode. With regard to process variable nodes, the numeric section of the label corresponds to a precise location in the application system. The precursor to the numeric section indicates the type of process variable the node represents. Examples of process variables include temperature, mass flow, pressure, and signals from sensors. Following the same order, these would be represented in nodes by the precursors T, M, P, and S.

Process variable deviations [**16**, **17**] are traditionally expressed as one of five discrete values: $+10$, $+1$, 0, -1, and -10; these correspond to large high, small high, normal, small low, and large low deviations. These values are also used to describe the effect a disturbance (e.g. failure mode) has on a particular variable. Two further values ($+5/-5$) are utilized during the development of the fuel rig system digraph to allow for the inclusion of partial failure modes. The causal relationships between process variable nodes remain as either non-acting, direct acting, or inverse acting. This component failure mode deviation addition leads to the effective application of digraphs in the fault diagnostics procedure involving the fuel rig system. The disturbances caused by complete failures, such as a pipe blockage or valve closure for example, are represented through utilizing the discrete variable '-10'.

A simple digraph is illustrated in Fig. 1. In the diagram it is noted that T1 and T2, the nodes, are connected by three edges. The alphanumeric code T1 represents temperature at location one. The edge with a gain of $+1$ is considered to be the normal edge since this represents the relationship which is 'usually true'. The second and third edges in the illustration are termed conditional edges since their relationship is only true whenever the condition represented by ':' exists. It must be noted that only one edge is true at any time.

A generalized procedure outlining the main steps involved in developing a system digraph is provided. The derivation of a digraph is well documented [**13**] and involves two basic steps.

1. *Step one: system analysis*. First, the system under investigation is defined. A specific number is allocated to each component thus developing a straightforward location reference approach for process variables and component failure modes at a given point. All relevant component failures

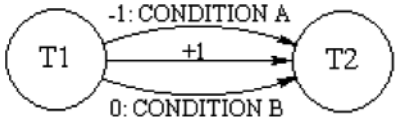

Fig. 1 Simple digraph representation

of the system are compiled with a failure mode code attached to each fault. The system is then separated into sub-units.

2. *Step two: digraph generation*. The unit digraph models for the sub-units, previously noted in step one, are generated. All process variable deviations that could have a potential effect on the variables in the model are taken into consideration. The system digraph is formed by connecting common variables from the sub-unit models.

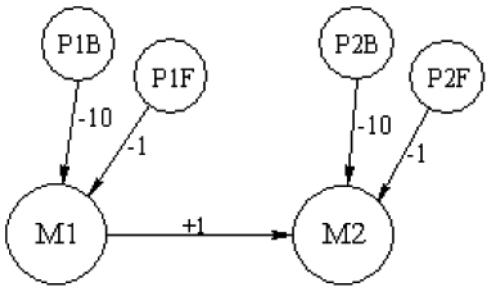

Fig. 2 Simple back-tracing example

3 SYSTEM FAULT DIAGNOSTICS STRATEGY

Emphasis is placed on the application of digraphs in the field of fault diagnostics. The fault diagnostics process is conducted using the system digraph model. System behaviour is monitored through compiling sensor data (e.g. via a level transmitter). In a given mode of operation the application system has a set of expected sensor readings. These are compared with the actual system readings during the diagnostic procedure to identify if any deviations are present.

1. *Step one: determination of system deviations*. The sensor readings which are expected while the system is in a known operating mode, for example mode ON, are noted. The current sensor readings from the system are retrieved and then compared with those expected, to determine if any deviations exist.
2. *Step two: flagging of non-deviations*. Non-deviating sensor nodes and associated digraph sections are 'flagged'. It is assumed that a non-deviating reading indicates the absence of a failure.
3. *Step three: back-tracing process*. Fault diagnosis involves back-tracing through the system digraph from a specific sensor node which represents the location of the given deviation. An unexpected process deviation within a system is represented by 'highlighting' the respective deviating node in the digraph. Subsequent propagation of the deviation through the system is conducted by marking all of the nodes which were affected by the initial highlighting. 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.

A simple back-tracing example is related to Fig. 2. It is assumed that a large negative deviation is registered at node M2, represented by M2(−10). Back-tracing thus commences from M2 to determine which failure modes may have contributed to the deviation. A single failure mode, P2B, is identified as directly influencing node M2. The failure mode P2F is disregarded since it results in a small negative disturbance on flow. The fault propagation is then followed to and ceases at node M1, where an additional failure mode (P1B) leading to a large negative deviation is determined. The back-tracing procedure therefore follows the route

$$\mathrm{M2}(-10) \rightarrow \mathrm{P2B}$$

$$\mathrm{M2}(-10) \rightarrow \mathrm{M1}(-10) \rightarrow \mathrm{P1B}$$

4 CASE STUDY

The feasibility of the fault diagnostic strategy is reviewed through application to a simulation test bed of an aircraft fuel system. The digraph technique is considered suitable for modelling the clear flow routes in the fuel rig system. As mentioned in the introduction, the purpose of a fuel system is reliably to provide an adequate amount of clean fuel at the right pressure to the engines during all phases of flight and manoeuvres. The fuel rig utilized incorporates a stainless steel frame supporting three active supply tanks. The complete configuration of the fuel rig is representative of a modern aircraft fuel system, illustrating the flow of fuel from the main and auxiliary tanks to the engine. The rig recreates the function of a general aircraft fuel system through using water instead of kerosene. The fault diagnostic strategy is tested across all modes of operation.

4.1 The fuel rig system

The general layout of the fuel rig is illustrated in Fig. 3. The three active supply tanks – main, wing, and collector – have two associated pump trays. Each tray encompasses a peristaltic pump, pressure relief valve, powered and manual isolation valves, and a pressure regulating valve.

The main tank represents the core group of tanks on an aircraft. Two pumps, connected in parallel, pump water from the main tank to the collector

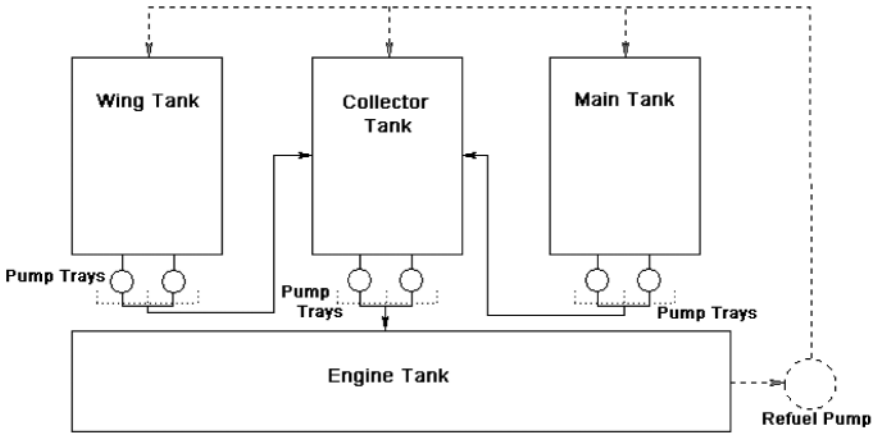

Fig. 3 General fuel rig layout

tank. The auxiliary storage tanks of an aircraft fuel system are represented by the wing tank. In a similar manner to the main tank, two parallel pumps transfer water from the wing tank to the collector tank. A large single tank at the base of the fuel rig represents an aircraft engine. Fuel feeding to the engine (represented by the engine tank) is conducted via fluid transfer from the collector tank through a pair of parallel connected pumps. A final pump, the centrifugal refuel pump, transfers water back into the active supply tanks from the engine tank. Complete drainage of the fuel rig system is conducted through utilizing the engine tank drain valve. The three active supply tanks are also connected to the engine tank via manually operated dump valves.

In order to monitor system behaviour and obtain the system status, data are retrieved from three types of sensors associated with the tank sections. Level, flow, and pressure transmitters are employed in the fuel rig system. The actual readings detected by the transmitters are classified into categories as follows.

1. Level transmitter: high, low, within normal boundary, pump shut-off, or empty. There are two additional levels associated with the collector tank; thresholds one and two are of relevance when considering the ACTIVE operating mode, as described next in section 4.1.1.
2. Pressure transmitter: pressure, no pressure, or partial pressure.
3. Flow transmitter: flow, no flow, or partial flow.

4.1.1 Modes of operation and component failure modes

There are three main modes of operation associated with the fuel rig system.

1. ACTIVE: fluid is transferred from the collector tank to the 'engine' (engine tank). The tank pumps are switched on, and powered isolation valves opened. As the collector tank level (CTL) decreases, fuel transfer from the wing and main tanks to the collector tank commences in the following manner.
   (a) Phase one: CTL above threshold one: no transfer from main and wing tanks.
   (b) Phase two: CTL below threshold one and above threshold two: transfer from wing tank only. If wing tank at 'pump shut-off', transfer from main tank.
   (c) Phase three: CTL below threshold one and above pump shut-off level: transfer from main tank given main tank level is above 'pump shut-off'.
2. DORMANT: system is in standby mode; no fuel transfer occurs between the active supply tanks and the engine. The tank pumps are switched off and powered isolation valves shut.
3. DRAIN: system is drained of fluid. Fuel transfer commences from the main, wing, and collector tanks to the engine tank via their specific drain valves.

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

Table 1 Component failure modes

Code*	Component failure mode
P_B	Pipe blocked
P_R	Pipe ruptured
P_PB	Pipe partially blocked
P_L	Pipe leakage
IVP_C	Powered isolation valve failed closed
IVP_B	Powered isolation valve blocked
IVP_O	Powered isolation valve failed open
IVP_PB	Powered isolation valve partially blocked
IVP_S	Powered isolation valve failed stuck
IVP_L	Powered isolation valve leakage
BP_B	Back pressure valve blocked
BP_PB	Back pressure valve partially blocked
BP_L	Back pressure valve leakage

* Where _ is replaced by the component ID number.

The peristaltic pumps, located in each active supply tank feed line, have four related failure modes, while the centrifugal pumps, utilized in both fuel transfer and refuel, have three. The pumps can fail on, shut off, or leaking. A further failure mode only associated with the peristaltic pumps involves a mechanical failure. There are two tank failure modes (tank ruptured or leaking) in addition to four possible pipe component failures (rupture, leakage, complete or partial blockage).

The component failure modes referenced in the modelling section (section 4.2) and their respective codes are highlighted in Table 1.

4.2 Modelling and diagnostic implementation

4.2.1 Fuel rig digraph development

Steps one and two from the digraph procedure, previously described in section 2, are used to develop the fuel rig system digraph. The system is split into four sub-units consisting of the main, wing, collector, and engine tank sections. Each section includes the actual tank and associated components. The respective sub-unit digraphs are joined at common process variables in order to form the overall system digraph. In total, the system digraph is constructed from 842 nodes, of which there are 151 process variable nodes and 691 component failure mode nodes. For a more detailed description of the development process involved in generating the fuel rig system digraph, the reader is directed to reference [**18**].

As a brief means of illustrating the development process involved in generating the fuel rig digraph, a detailed section of the main tank is depicted in Fig. 4. The main tank pump trays incorporating two powered isolation valves (IVP0110/IVP0120), back pressure valves (BP0110/BP0120), a flow transmitter (FT0110), and interconnecting pipe work are illustrated.

A section of the respective main tank digraph is presented in Fig. 5. The alphanumeric codes contained

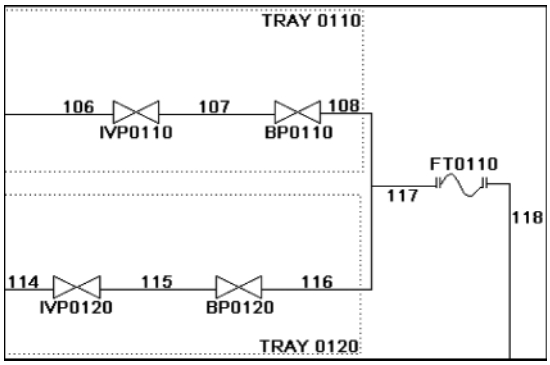

Fig. 4 Main tank section

within the digraph nodes represent system process variables and component failure modes, as previously described in section 2. The fuel mass flow in trays 0110 and 0120 is indicated by the routes incorporating nodes M106→M108 and M114→M116 respectively. The two mass flow paths are connected by an AND gate (vertical line) before leading to node M117. This represents the joining of the tray lines at pipe 117. The component failure modes considered to affect the functionality of the fuel rig system are identifiable in Fig. 5 through the manner in which they feed into their associated process variable nodes.

The relationship between M106 and M107 represents the powered isolation valve IVP0110. If the valve is closed by the operator then the relationship (0: IVP110C) between the two mass flow nodes is nullified. Similarly, the back pressure valve BP0110 is represented by the '+1' edge joining M107 with M108. The mass flow nodes have at least four associated failure modes which are related to four identified pipe faults: partial or complete blockage, rupture, or leakage. Additional failure modes are dependent on the presence of further components, such as valves.

4.2.2 System fault diagnostics

In order to enable a more thorough system investigation, consideration of dynamic effects is required. The main area of focus when considering system dynamics relates to abrupt fault analysis [**19**]. Abrupt faults represent dramatic changes in a system and can therefore result in a significant visible deviation, known as a transient, from the normal system operating mode. In time, the system can be observed moving into a new 'steady state' owing to the deviation. This is synonymous with the fuel rig system changing scenario when assumed to be in one of the operating modes. The term 'scenario' in the fuel rig analysis relates to an altered system status based on the retrieved transmitter readings.

A necessary strategy is to analyse system behaviour at frequent intervals in order to perform diagnostics

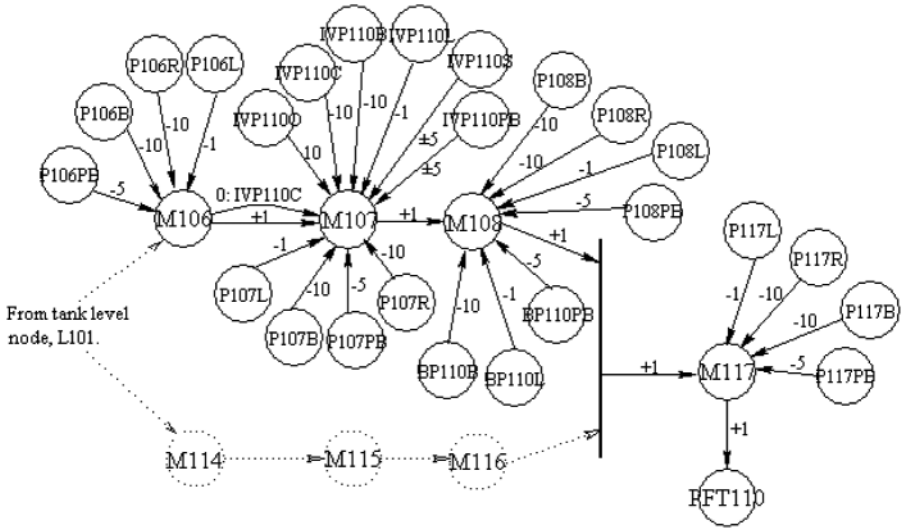

Fig. 5 Section of main tank digraph

and identify if the system has shifted from its normal operating mode. This strategy involves monitoring the fuel rig system and determining if the system is in an abnormal scenario. This does not, however, include scenarios that would be expected during fault rectification. Data are retrieved according to a set sampling rate. The dynamic effects of faults are investigated through the monitoring of tank levels, in particular the rate of change in levels.

The following statements are assumed during the diagnostics procedure.

1. All transmitters provide reliable readings.
2. For full flow and no flow registered deviations at the flow transmitters FT0110 (main tank), FT0210 (wing tank), or FT0310 (collector tank) a fault must have occurred in both tank feed lines. The transmitters are located at the flow exit points from each tank section.
3. For partial or minor flow deviations, of gains ±5 or −1, a failure must have occurred in at least one of the tank feed lines.

The diagnostic program, coded in MATLAB, can be subdivided into four main sections, namely input, comparison, fault diagnostics, and output. During the 'input' stage the individual fuel rig transmitter readings and assumed operating mode of the fuel rig are 'read into' the program by way of a text file.

The expected fuel rig operating mode state is determined in the 'comparison' section through considering the individual tank levels. Should the fuel rig be in the ACTIVE mode then the collector tank level is used in order to determine which ACTIVE phase, as detailed in section 4.1.1. Specific rules are employed for all of the operational modes as a means of providing consistency. These rules relate to the tank levels and in turn the flow readings that would be permissible for a given situation. The expected readings for a known operating mode may therefore be altered depending on the level information.

1. If any tank level is at or below pump shut-off (PSO) level, expect readings of no flow and no pressure at the respective flow and pressure transmitters in the tank section.
2. If the CTL is high, expect no flow out of the main and wing tanks.
3. If there is flow out of a tank (via pipes) and the level is below PSO, all failures are assumed to result from the flow out, not an actual tank failure (e.g. fracture).

A deviation matrix [**D**] is formed at the end of the 'comparison' phase by comparing the retrieved transmitter data with those readings expected under the assumed fuel rig system operating mode. For identical readings, an element in the deviation matrix that corresponds to the relevant transmitter is allocated the value '0'. This indicates the presence of a non-deviating sensor and it is assumed no failures are present in the corresponding specific section of the fuel rig. For deviating readings a respective element in [**D**] is assigned a value which is consistent with the noted deviation (e.g. +10). On generating the deviation matrix the next phase in the process revolves around determining transmitter flags for non-deviating readings. This is split into two steps: first, whole tank section flags and, second, individual transmitter flags.

The back-tracing procedure is re-enacted through using matrices which contain the individual component failure mode results for a given transmitter deviation. The number of flags signed '1', representing system deviations for given tank sections and transmitters, dictates which back-tracing results should be ANDed.

The tank level data are used to calculate the rate of change in the fuel rig tank levels. These calculations are performed after data are retrieved from the second sampling interval. The rate of change in tank heights is used during the 'fault diagnostics' section. For specific cases where no flow is registered in the tank feed lines, then the rate of change in tank level is utilized to determine whether there has been a pipe blockage (or valve closure/pump shut-down) or pipe rupture. A rupture, unlike a blockage, would lead to a decreasing tank level.

Each fuel rig tank section is linked to specific output text files which contain the diagnostic results for the given transmitter deviations. From engineering knowledge, it is assumed more probable for fault combinations of the lowest order to be the cause for a noted set of deviations.

4.2.3 Results obtained for a given dynamic scenario

The transmitter data presented in Table 2 contain a sample from a set of readings retrieved over intervals of 30 s. The fuel rig is assumed to be set in the ACTIVE mode. Given that the height of the CTL is less than threshold one but greater than threshold two, fluid transfer is expected to flow from the wing tank to the collector tank (ACTIVE phase two). The expected system readings are illustrated above the retrieved transmitter interval data. The actual data exhibit a single deviation (highlighted in bold in Table 2) in the wing tank section. The codes contained within Table 2 are defined in the associated table key.

Upon reading the retrieved operational data from the fuel rig into the program, results are output for each interval. For intervals 1 and 2 the presence of a single deviation in the wing tank and the absence of deviations in the main and collector tank sections are noted. The flow transmitter FT0210 detects the deviation 'no flow', however, the expected operating mode readings are recorded by the pressure transmitters PT0110 and PT0120. From the given deviation, the diagnostic program assumes faults are present in a section of the wing tank incorporating the feed lines between transmitters FT0210 and PT0110/PT0120. The results are output in two text files: one outlines the multiple faults achieved when back-tracing from the flow transmitter node past the 'AND' gate in the digraph through both tank feed lines (results for each line are ANDed); the second highlights the single failure causes located in the wing tank section between the joining of the two feed lines and the flow transmitter. In total, 83 failure causes are noted for the wing tank section deviations – two first order and 81 second order.

Through taking into consideration the 'static' wing tank level recorded between intervals one and two, it is feasible to reduce the number of failure combinations yielded for the given scenario. The rate of change in height of the wing tank level is used to distinguish between and 'hone in on' failures that may be the cause for the noted 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 FT0210 would suggest the presence of rupture faults. Taking the rate of level change into account generates 37 failure combinations – one first order and 36 second order – as illustrated in Table 3. The noted failures are associated with pipe or valve blockages (P__B, BP__B, IVP__B) and valve closures (IVP__C).

As a means for establishing the most probable cause of failure, reliability theory regarding unavailability functions and importance measures is utilized in order to rank the failure combinations yielded for a deviating scenario. Generic failure rate data are obtained in order to quantify the unavailability of relevant fuel system components for a given scenario. The ranking of the failure combinations is determined through application of the Fussell–Vesely probabilistic measure of minimal cut set importance. The potential failure cause combinations (cut sets) are given a numerical rating, with the highest being deemed the most likely cause of failure. The importance measure is defined as the probability of occurrence of a cut set given that the system has failed in its deviated state (Q_{SYS}). Q_{SYS} is calculated using the

Table 2 Fuel rig transmitter data

	Main tank				Wing tank				Collector tank			
Assumed ACTIVE mode	Level	Drain flow	Feed line flow	Feed line pressure	Level	Drain flow	Feed line flow	Feed line pressure	Level	Drain flow	Feed line flow	Feed line pressure
ACTIVE	RL	NF	NF	NP	< RL & > PSO	NF	F	P	< T1 & > T2	NF	F	P
Interval 1	RL	NF	NF	NP	< RL & > PSO	NF	**NF**	P	< T1 & > T2	NF	F	P
Interval 2	RL	NF	NF	NP	< RL & > PSO	NF	**NF**	P	< T1 & > T2	NF	F	P

NF = no flow; NP = no pressure; T1 = threshold one; F = flow; P = pressure; T2 = threshold two; PF = partial flow; RL = required level; and PSO = pump shut-off.

rare event approximation as opposed to calculating an exact value. No difference has been noted in the ranking of the cut sets when considering either the rare event or exact values for Q_{SYS}. Furthermore, for cases whereby many cut sets are produced, it is computationally demanding to determine an exact value for Q_{SYS}.

For the results noted in Table 3, the top five ranked failures and their respective numerical ratings are:

(a) P217B: 0.940;
(b) IVP210B.IVP220B: 0.020;
(c) BP210B.IVP220B: 0.015;
(d) IVP210B.BP220B: 0.015;
(e) BP210B.BP220B: 0.011.

For the given deviating scenario, a manual isolation valve located in pipe 217 in the fuel rig test bed was closed as a means of simulating a pipe blockage. It is noted that the actual injected fault (P217B) is ranked at the top of the retrieved failure list. In addition to the ranking procedure, final human intervention with the ability to call on engineering knowledge and experience will target the most probable failure modes.

Table 3 Wing-tank section fault diagnostic results

Single failure	P217B
	OR
Multiple failure (a)	P209B, BP210B, P208B, IVP210B, IVP0210C, P207B
	AND
Multiple failure (b)	P216B, BP220B, P215B, IVP0220C, IVP0220B, P214B

5 DISCUSSION

As a means for determining the effectiveness of the application of digraphs in fault diagnostics, failures are injected into the fuel rig system. The fuel rig operator is able to override manually specific functions and thus simulate scenarios which are altered from the normal operating mode of the system. For example, it is possible to close a manual valve in one of the tank feed lines so as to replicate a pipe blockage situation. The retrieved fuel rig readings are then compared with those expected in order to determine the component failure modes that may have led to the registered deviation(s). Having the ability to inject faults into the system yields the capacity to test the diagnostic strategy thoroughly. Table 4 illustrates the deviations associated with five fuel rig test cases. The actual injected fault(s) and the number of failure modes determined are also highlighted. It is noted that for all of the test cases the actual injected fault is generated as a probable cause.

The key issue with the diagnostic strategy lies within distinguishability. Numerous fault options may be retrieved for a given scenario. During these cases, reliability theory and human knowledge have to be called upon in order to highlight the 'most probable' cause. 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.

Table 4 Fuel rig scenario results

Test case	Injected fault(s)	Registered deviations	No. of faults determined
1	*Main tank* Both tray powered isolation valves open Both tray peristaltic pumps on	*Main tank* Feed line flow transmitter: Flow Feed line pressure transmitter: Pressure	16: 1 second order 6 third order 9 fourth order
2	*Wing tank* Pipe rupture at location 217 (open globe valve to simulate)	*Wing tank* Feed line flow transmitter: No flow	10: 1 first order 9 second order
3	*Main tank* Tank rupture (open main tank drain valve to simulate)	*Main tank* Level transmitter: Decreasing level	2: 2 first order
4	*Main tank* Tank rupture	*Main tank* Level transmitter: Decreasing level	2 (main tank): 2 first order 49 (collector tank):
	Collector tank Single tray powered isolation valve shut	*Collector tank* Feed line flow transmitter: Partial flow	13 first order 36 second order
5	*Main tank* Both tray powered isolation valves open Both tray peristaltic pumps on	*Main tank* Feed line flow transmitter: Flow Feed line pressure transmitter: Pressure	16 (main tank): 1 second order 6 third order 9 fourth order
	Collector tank Single tray powered isolation valve shut	*Collector tank* Feed line flow transmitter: Partial flow	49 (collector tank): 13 first order 36 second order

The readings obtained from the fuel rig system are subdivided into categories depending on the transmitter variable under investigation. In order to overcome the issue regarding the sensitivity of fuel rig transmitter readings to high-frequency influences such as noise, set boundaries are constructed for normal pressure (or flow), no pressure (or no flow), and partial pressure (or partial flow). Thresholds for the level, flow, and pressure readings are determined so as to prevent 'false alarms' with regards to registered deviations.

Digraphs provide a suitable method for representing relationships between entities, and are considered a useful tool in modelling the information flow within systems. It is this characteristic which makes digraphs appropriate for the fuel rig case study. While conducting testing no discrepancies were noted between the digraph model and physical system under investigation. This can be attributed to the fact that the fuel rig system digraph is developed from a detailed piping and instrumentation illustration. Discrepancies may be evident if numerous system variables (e.g. mass flow, temperature) are to be taken into account at a given location in the digraph model.

On dealing chiefly with mass flow relationships in the fuel rig digraph, the diagnostic back-tracing procedure is sufficient for the given system since transmitter readings are taken downstream of prospective failure locations. It may, however, be necessary to consider 'forward-tracing' when reviewing applications with numerous complex relationships which span across subsystems. The incorporation of 'flagging' into the diagnostics process eradicates the potential for inconsistent failure mode results and anomalies. 'Flagging' therefore acts as a form of consistency check and removes the possibility of conflicting results between non-deviating transmitter nodes and failure modes yielded through back-tracing from specific deviating nodes. This process is adapted when considering the dynamics of a system. For scenarios whereby a tank level is noted to be within an abnormal boundary in consecutive intervals, if the rate of change in height of the tank level is a non-negative value, it is assumed that the tank failure has been rectified and therefore the deviation is masked. For example, consider a low wing tank level with a decreasing rate of change in the first interval. If the tank failure is rectified, a low level is still likely to be retrieved in the second interval. The low level is, however, considered a non-deviation.

The current application system does not incorporate an integrated control loop structure. Adaptations are conducted on the main tank section of the fuel rig to assess the viability of both modelling systems (and their associated control loops) and performing fault diagnostics from the resulting digraph. A level control system, consisting of two negative feedforward loops, is incorporated into the main tank. The digraph, generated for the revised main tank section, successfully models the process flow structure of the system under investigation, and thus application of the digraph-based diagnostic strategy is feasible. Preliminary research is encouraging, with regard to the determined back-tracing results when considering both reliable and unreliable level switches and control units.

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. On application of the method to an actual aircraft fuel system, it is felt that individual digraphs are to be developed for specific operating modes in order to prevent the generation of unwieldy models. The application of the digraph models in the fault diagnostics process for each operating mode will thus be conducted separately. It will, however, be necessary to verify the models through conducting analytical testing.

To address the issues raised in the introduction regarding fuel systems, modelling of the fuel storage and distribution sections is conducted using nodes representing mass flow. The edges which connect the nodes indicate the mass flow routes within the system. It is unclear whether digraphs are suited to modelling other aircraft systems, more specifically the avionics sections. The flight management system (FMS) is considered an avionics component, the primary function of which is to assist pilots in planning, navigation, and aircraft control functions. The range and variety of data that must be taken into account imply that it may be difficult to represent the associated data using the standard notation for nodes and edges. A method for overcoming this noted limitation is likely to involve the employment of unique nodes and connection types.

6 CONCLUSIONS

Digraphs provide a clear representation of the relationships between system variables since they closely reflect the physical structure of the system under investigation. The discrete values used to describe the relationships between nodes have proved to be sufficient with the addition of '$+/-5$' enabling the introduction of partial failures. This adaptation overcomes one of the noted limitations of the established digraph development procedure with regard to the misrepresentation of some variable relationships. Given the relatively straight forward transfer of fluid process of the fuel system, discrepancies between the model of system behaviour using the digraph and the actual behaviour have been

minimal and easily eradicated via testing. Models for other systems may require a more detailed verification process.

The rate of change in height of a particular tank level is utilized to distinguish between and 'hone in on' failures that may be the cause for a given deviation. This has proved successful in cases where there are registered deviations of no flow and no pressure. A noted negative rate of change highlights pipe rupture faults. Conversely, a positive or zero rate of change indicates the presence of faults incorporating blockages or closures. A mechanism to further identify the 'most likely' causes of a registered deviation is required. Focus is to be based on the weighting of failure modes through using previous data from maintenance logs. There is also the provision to investigate the importance of the type and location of transmitters providing relevant system information. Issues associated with the fault diagnostic strategy have been addressed and detailed in the previous (discussion) section.

The results from the application of the automated diagnostics process, based on the digraph method, to the fuel rig system have been proven to be credible. Injecting faults into the fuel rig has allowed various scenarios to be tested using the diagnostic method. Valid failure mode results are obtained when considering single or multiple faults in either individual tank sections of the fuel rig or across the whole system. This in turn leads to the applicability of the method in a complex system comprising an actual aircraft fuel system.

ACKNOWLEDGEMENTS

The authors wish to thank Dr J. Pearson from the Systems Engineering Innovation Centre (SEIC), BAE Systems for information provided on the fuel rig system.

REFERENCES

1 **Papadopoulos, Y.** and **McDermid, J.** Automated safety monitoring: A review and classification of methods. *Int. J. Condition Monitoring and Diagnostic Engng Mgmt*, 2001, **4**(4), 1.

2 **Novak, F., Žužek, A.,** and **Biasizzo, A.** Sequential diagnosis tool. *Microprocessors and Microsystems*, 2000, **24**(4), 191.

3 **Shakeri, M., Raghaven, V., Pattipati, K. R.,** and **Patterson-Hine, A.** Sequential testing algorithms for multiple fault diagnosis. *IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans*, 2000, **30**(1), 1.

4 **Price, C.** AutoSteve: electrical design analysis. *Colloquium Digest – IEE*, 1997, **338**(4), 60.

5 **Price, C.** and **Taylor, N.** Multiple fault diagnosis from FMEA. In Proceedings from the National Conference on *Artificial intelligence*, Rhode Island, USA 27–31 July 1997, pp. 1052.

6 **Papadopoulos, Y., Parker, D.,** and **Grante, C.** Automating the failure modes and effects analysis of safety critical systems. In Proceedings of the Eighth IEEE Symposium on *High assurance systems engineering*, Tampa, USA, 25–26 March 2004, pp. 310.

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

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

9 **Rao, N. S. V.** Expected-value analysis of two single fault diagnosis algorithms. *IEEE Trans. Computers*, 1993, **42**(3), 272.

10 **Iverson, D. L.** and **Pattersine-Hine, F. A.** Advances in digraph model processing applied to automated monitoring and diagnosis. *Reliability Engng and System Safety*, 1995, **49**(3), 325.

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

12 **Kohda, T.** and **Henley, E.** On digraphs, fault trees and cut sets. *Reliability Engng and System Safety*, 1988, **20**(1), 35.

13 **Venkatasubramanian, V., Rengaswamy, R., Yin, K.,** and **Kavuri, S. N.** A review of process fault detection and diagnosis, Part II: Qualitative models and search strategies. *Computers and Chem. Engng*, 2003, **27**(3), 313.

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

15 **Maurya, M. R., Rengaswamy, R.,** and **Venkatasubramanian, V.** A systematic framework for the development and analysis of signed digraphs for chemical processes. 2. Control loops and flowsheet analysis. *Ind. and Chem. Engng Res.*, 2003, **42**(20), 4811.

16 **Andrews, J.** and **Brennan, G.** Application of the digraph method of fault tree construction to a complex control configuration. *Reliability Engng and System Safety*, 1990, **28**(3), 357.

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

18 **Kelly, E.** and **Bartlett, L. M.** Aircraft fuel system diagnostics using digraphs. In Proceedings of the 19th International Conference on *Condition monitoring and diagnostic engineering management* (*COMADEM*), Luleå, Sweden, 12–15 June 2006, pp. 44.

19 **Mosterman, P. J.** and **Biswas, G.** Diagnosis of continuous valued systems in transient operating conditions. *IEEE Trans. Systems, Man. and Cybernetics, Part A: Systems and Humans*, 1999, **29**(6), 554.