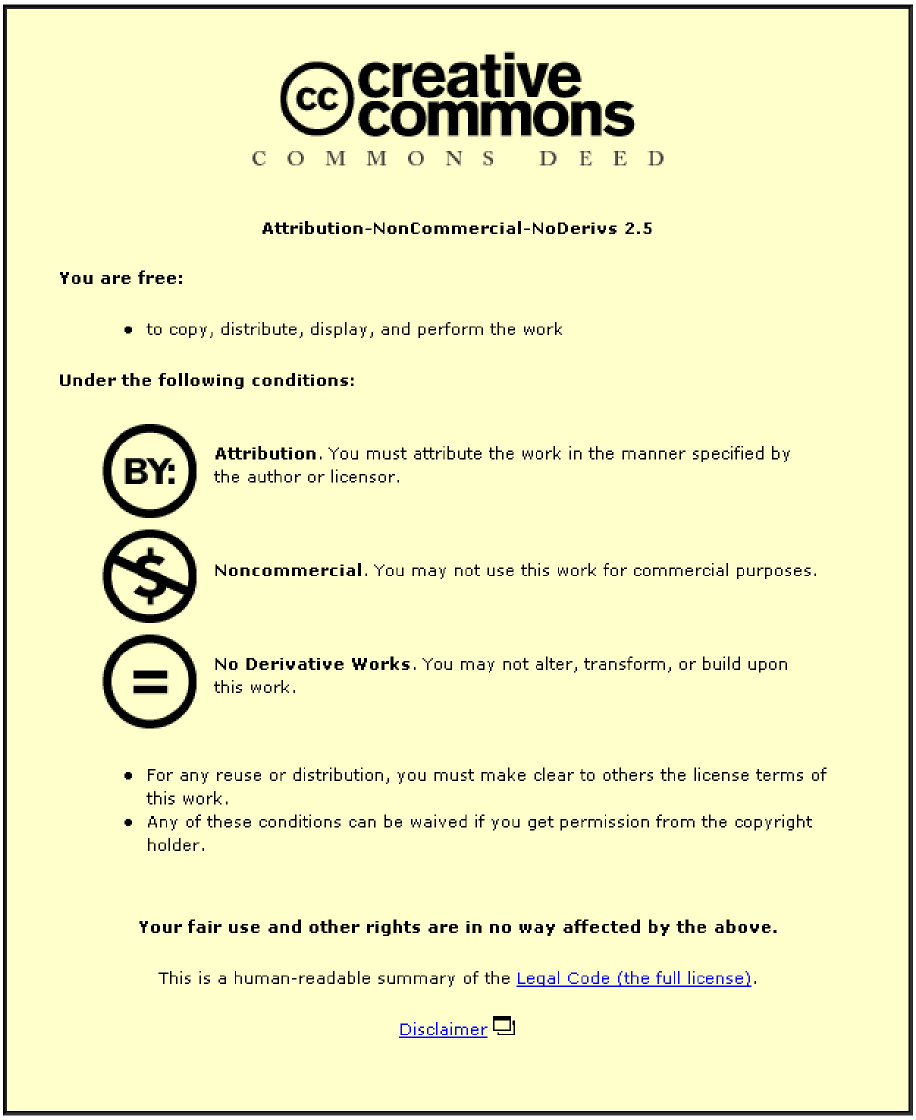


Citation: Hurdle, E.E., Bartlett, L.M. and Andrews, J.D., 2007. Fault tree based fault diagnostics methodology for an aircraft fuel system. IN: Proceedings of the 32nd ESREDA Seminar: Maintenance Modelling and Applications, 8-9th May, Hotel dei Pini, Località Le Bombarde – Alghero (SS).
This is a pre-publication version.

Fault Tree Based Fault Diagnostics Methodology for an Aircraft Fuel System

E. E. Hurdle, L. M. Bartlett and J. D. Andrews
Department of Aeronautical and Automotive Engineering,
Loughborough University,
Loughborough,
LE11 3TU,
England,
United Kingdom

Abstract

For aircraft the possibility of avoiding cancellations and delays can be considerably improved by reducing the time taken to restore systems to the working state when faults occur. The fault identification process can be a significant proportion of the time taken in the repair process. Having diagnosed the problem the restoration of the system back to its fully functioning condition can then take place.

This paper describes the development of a fault diagnostic methodology for an aircraft fuel system. The approach takes into account the dynamics of the system. Using sensors installed to provide information about the current status of certain critical parameters. The information produced for these parameters are then categorised into different trend types using a simple pattern recognition technique. Non-coherent fault trees are then used to identify all possible causes of the observed sensor reading trends. By combining the information provided from all sensors the causal faults can be detected. The approach presented has been developed and tested for small demonstration systems – this paper describes how it has been scaled up for a larger, more representative system and the issues that have been overcome in doing this. The system used exists as an experimental facility where the procedure developed can now be fully tested.

Keywords: Fault Detection and Diagnosis, Fault Tree Analysis

1. Introduction

Advances in technology have resulted in the increasing complexity of contemporary systems and in turn brought about an ever-growing need for improved fault detection and diagnostic techniques. The quicker a failure can be detected and identified within a system the sooner measures can be made to replace or repair the component and return the system to normal operation. This will enable the system to function for a longer period of time, therefore increasing company profitability. A failure that is left undetected could lead to the occurrence of other problems in the system and longer down-time from normal operation.

A number of approaches to diagnosing faults in systems have looked at the diagnosis of single failures. For instance, Novak and his research team have developed a sequential diagnostic tool that uses the symptoms from the system in order to determine its status by carrying out a series of tests [1-4]. The method only takes into consideration single failures and so is not able to address the issue of several failures occurring at the same time. The symptoms that then occur in the system may differ completely to those exhibited when each fault individually occurs. Sequential testing was extended to account for multiple failures by Shakeri et al. [5], but further research is required to consider redundancy and unreliable sensor readings.

Previous research has been carried out using a fault tree based method to address the issue of identifying multiple failures within a system. Fault trees are used to explain the deviations from normal operation observed in the sensor outputs, and a non-coherent tree structure was found to be the most effective [6, 7]. Further expansion to this work has looked at incorporating dynamic effects into the methodology using a simple pattern recognition process [7-9].

A dynamic method for diagnosing single and multiple faults in systems using fault tree analysis has been demonstrated by applying it to a simple water tank level control system [9]. An important issue highlighted in previous work was the scalability of the method for use on larger and more complex models. Also how redundancy in the system is handled needs to be established. This paper describes the extension of the dynamic method by applying it a model based on a fuel rig from BAE Systems. This system features redundancy and is a larger system than those previously considered.

2. Dynamic Fault Detection and Identification Process

The dynamic fault detection and identification process is categorised into two stages, these being 'modelling and preparation' and 'application'. The modelling and preparation stage is the part of the analysis in which all available information about the system is collected. This information is then used in the application stage in order to ascertain the cause of failure from symptoms exhibited on the system. The stages are described in more detail in Sections 2.1 and 2.2 respectively.

2.1 Modelling and Preparation Stage

1. The system is first divided up into sub-systems. The sub-systems are parts of the system that provide a function and yield an input, and/or obtain an output from another sub-system.

2. The sub-system process variables that are to be measured, such as flow, temperature, pressure or level are identified. Sensors are then incorporated into the system to monitor these variables if not already present for control purposes.

3. Key locations of the measured process variables in each sub-system and therefore for the overall system are identified. These locations will be those points where a change in normal control action will initially become apparent.

4. All the possible modes of system operation at any point in time are listed. Modes of operation may also be divided further into appropriate ‘sub-modes’ in the event that its complexity is too difficult to deal with on its own. Assumptions to be made that can affect the operation of the system are identified.

5. For each of the system operating modes identified, a set of potential patterns from the readings obtained for the key measured variables are developed. Any potential behaviour for individual sub-modes if used in the analysis of a specified mode is also included.

6. For each sub-system the potential pattern behaviour for any other transmitter readings that can be taken are identified. Again, if sub-modes are used then identify the possible behaviour for each of these.

7. Fault trees for causes of the observed trends in the process variables at each of the sensor locations in the system are drawn. Each fault tree is developed down to the component failures in the system. Fault trees may be drawn for absolute values or rates of change, depending on what information is considered useful for the particular system. For any normal system behaviour causes of sensor readings are developed using success trees, which describe all the components in the system that must be working correctly in order for that outcome to occur.

2.2 Application Stage

1. Pattern recognition techniques are used to identify the actual patterns obtained for system sensor readings. These are then compared to those for the expected behaviour. If these patterns match this indicates the system is working as it should be for the given mode or sub-mode. Any pattern that does not match up with this behaviour is indicative of a failure of some kind within the system. There may be hidden failures, but these would only become apparent through moving into a different sub-mode during system operation, or by switching the operating mode.

2. Sub-systems of the overall system with the potential to have caused the observed symptoms resulting in the incorrect patterns from the key variable transmitters are identified.

3. Each identified sub-system is then investigated in turn and the actual patterns from readings for all the transmitters in that section checked against those expected. Fault trees are constructed for both the deviated and successful patterns for the sub-system. These causes of readings are combined using an AND gate with the status of certain basic events being determined by the transmitter patterns.

4. A list of prime implicants (combinations of component states, working and failed, that produce the indicated patterns) will be obtained from the combined fault tree for each sub-system. A coherent approximation is then made by assuming that all working states are TRUE in order to obtain a list of cut sets (failed component states that produce the indicated patterns).

5. The cut set list obtained is then minimised in order to produce a list of the potential causes of failure for the specified sub-system.

6. If there is more than one potential cause of failure then importance measures can be used to rank the failure modes using their probability of occurrence in order to determine the most likely outcome.

The process described is now demonstrated by applying it to a representation of an aircraft fuel supply system. This system exists as an experimental fuel rig, located at BAE Systems.

3. Example System Application

The aim of any aircraft fuel system is to provide an adequate supply of clean fuel at an appropriate pressure level to all the engines throughout the flight phase. The fuel rig system, illustrated in Figure 1 is a model representing a real aircraft fuel system that uses water to simulate the fuel flow. The rig consists of three tanks; main, wing and collector in which water is distributed to the engine feed.

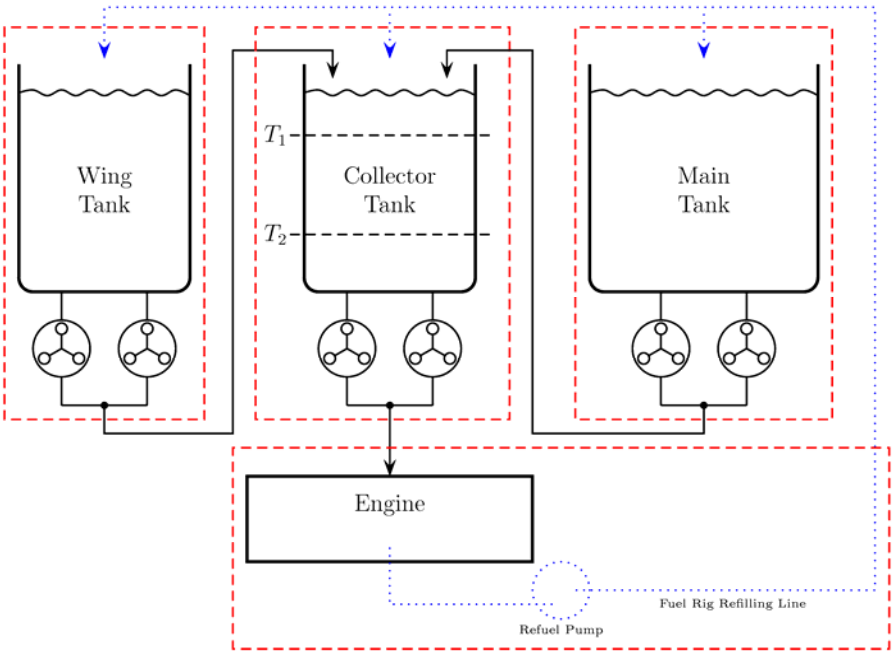


Figure 1. The fuel rig system.

Each tank has two pump trains, each containing a peristaltic pump (PP), pressure sprung relief valve (PSV), powered isolation valve (IVP) controlled by a controller (CT), back pressure valve (BP) and connecting pipe work (P). This is shown in more detail for the main tank section in Figure 2. The two fuel line streams out of each tank are labelled ‘Line L1’ and ‘Line L2’. These join up to become the main outflow line out of the tank. Either of the two lines can be used when fuel is required, but fuel is only drawn out of one line from each tank at any point in time, the second is left in a standby mode, thus providing the system with redundancy.

When the engine is switched on all peristaltic pumps turn on, including those on lines that are on standby. When fuel is not required from a line the powered isolation valve remains closed, and the water is re-circulated back into the tank via the overflow line, as shown in more detail for a single tank section (this being for the main tank) in Figure 2. The fluid flow along each overflow line is regulated by a pressure relief valve.

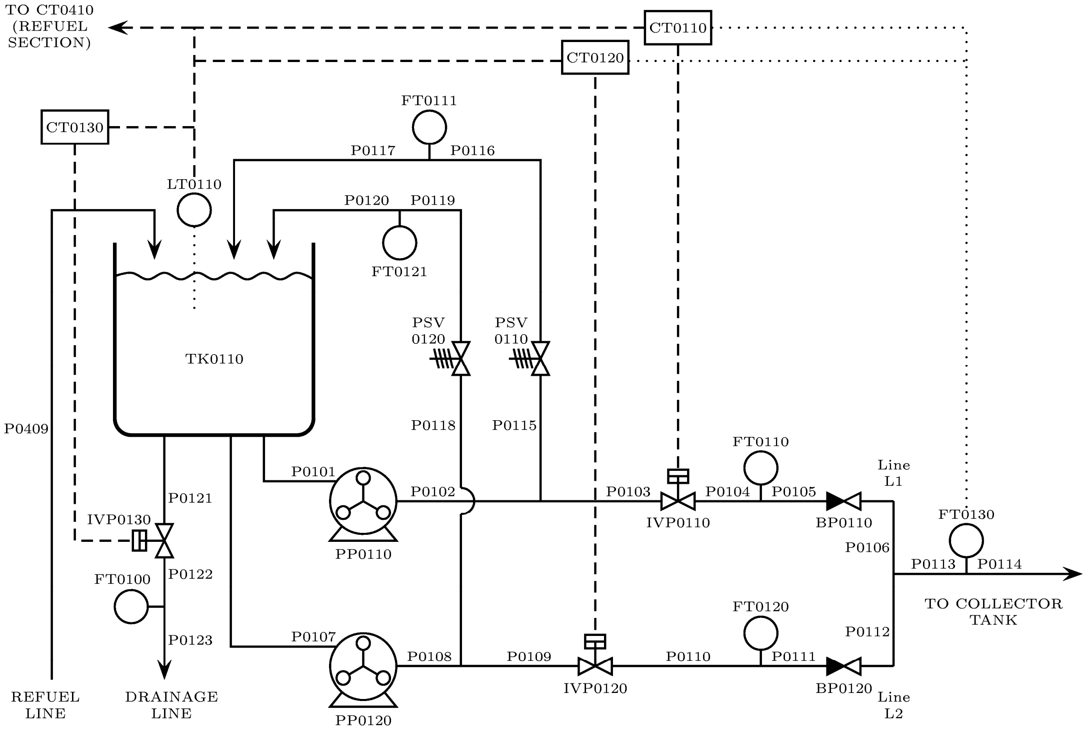


Figure 2. The main tank sub-system.

Water is fed only to the engine from the collector tank. Both main and wing tanks are used to feed the collector tank when the level of water drops below a designated threshold. The wing tank, which simulates the auxiliary fuel storage in the system, is used for replenishing the collector tank when the level of water drops to or below threshold T_1. Once the supply of water from the wing tank has been used and/or the level in the collector tank drops to or below threshold T_2 fluid will then be fed from the main tank, which simulates the main fuel storage in an aircraft system. It is assumed that under normal operating conditions water is pumped into the collector tank at the same rate as it is pumped out into the engine. Therefore the water level in the collector tank will increase as a result of a failure in the system.

The engine in the fuel rig system is represented by a large tank located at the base of the rig. This collects the water from the system, indicating that the fuel is being successfully fed out and into the engine. This part of the rig is also used to represent the refuelling of an aircraft. The refuelling area is indicated in Figure 1 using a dotted line. Once a run has taken place the water in the engine tank is pumped back into the appropriate other three tanks via a centrifugal refuel pump.

The main, wing and collector tanks each have a valve for drainage controlled by a controller, which may be used to represent the dumping of fuel from an aircraft. In this case the main and wing fuel lines are shut down and both these tanks are drained of water to pump shut off. The collector tank is also drained to a low level, leaving enough fuel for landing. The water from all the tanks is drained into the engine tank in the rig so that it can be redistributed back into the system.

The system has two main modes of operation; these being ‘ACTIVE’ when fluid is pumped from the collector tank to the engine, or ‘DORMANT’ when all the pumps are shut down and there is no fluid transfer. In the ACTIVE operating mode as the transfer of water between the collector tank and the engine takes place the level of water in the collector tank decreases. This is replaced by water being transferred, initially from the wing and then later on from the main tank. In the DORMANT operating mode the system is in a standby function with all powered isolation valves remaining closed and the peristaltic pumps turned off. Therefore no fluid transfer is expected to take place in this case.

There are two additional operating modes that the system can be in, which are ‘FUEL DUMPING’ or ‘REFUELLING’. In the FUEL DUMPING mode the pumps in the main and wing tanks are shut down and corresponding powered isolation valves are closed (in effect becoming DORMANT). Water is drained from each of these tanks to the pump shut off point. The level of water in the collector tank is drained to level low in order to leave enough fuel for landing. Drainage of each tank takes place through the drain valves, located on the drainage lines.

In the REFUELLING mode the system is effectively DORMANT with the water levels of the main, wing and collector tanks initially at any level. The 3 tanks are refilled with water to the required level if they are below this. In fuel rig the engine tank is used to simulate an aircraft refuelling tanker. Water is pumped from this tank into the other three tanks. All the peristaltic pumps in the system are shut down and the powered isolation valves on the lines out of the main, wing and collector tanks remain closed.

In order to apply fault tree analysis to any system all possible failures that could occur for each of the system components must be defined. Table I contains a list of possible component failures and their code for the main, wing and collector tanks in the system. The example used to show the method in this paper does not use the refuelling section in the system; therefore the potential of failure for this part of the system is omitted.

Table I: Potential component failures for the main, wing and collector tanks in the fuel rig system.

Code	**Component Failure**
IVP0ij0FC ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 Fails Closed
IVP0ij0FO ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 Fails Open
IVP0ij0FS ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 Fails Stuck
IVP0ij0B ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 is Blocked
IVP0ij0PB ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 is Partially Blocked
IVP0ij0L ($1 \leq i \leq 3$) ($1 \leq j \leq 3$)	Powered Isolation Valve IVP0ij0 is Leaking
PSV0ij0ISC ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 is Incorrectly Set Closed
PSV0ij0ISO ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 is Incorrectly Set Closed
PSV0ij0FS ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 Fails Stuck
PSV0ij0B ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 is Blocked
PSV0ij0PB ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 is Partially Blocked
PSV0ij0L ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Pressure Sprung Relief Valve PSV0ij0 is Leaking
BP0ij0B ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Back Pressure Valve BP0ij0 is Blocked
BP0ij0PB ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Back Pressure Valve BP0ij0 is Partially Blocked
BP0ij0L ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Back Pressure Valve BP0ij0 is Leaking
PP0ij0FSO ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Peristaltic Pump PP0ij0 Fails Shut Off
PP0ij0FO ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Peristaltic Pump PP0ij0 Fails On
PP0ij0FM ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Peristaltic Pump PP0ij0 Fails Mechanically
PP0ij0L ($1 \leq i \leq 3$) ($1 \leq j \leq 2$)	Peristaltic Pump PP0ij0 is Leaking
P0$ij$B ($1 \leq i \leq 3$) ($01 \leq j \leq 23$)	Pipe P0$ij$B is Blocked
P0$ij$F ($1 \leq i \leq 3$) ($01 \leq j \leq 23$)	Pipe P0$ij$B is Fractured
P0ijPB ($1 \leq i \leq 3$) ($01 \leq j \leq 23$)	Pipe P0$ij$B is Partially Blocked
P0$ij$L ($1 \leq i \leq 3$) ($01 \leq j \leq 23$)	Pipe P0$ij$B is Leaking
TK0ij0R ($1 \leq i \leq 3$)	Tank TK0ij0 has Ruptured
TK0ij0L ($1 \leq i \leq 3$)	Tank TK0ij0 is Leaking
CT0ij0T ($1 \leq i \leq 3$)	Controller CT0ij0 Fails Reading TRUE
CT0ij0F ($1 \leq i \leq 3$)	Controller CT0ij0 Fails Reading FALSE

The subscript ‘i’ represents the particular sub-system and ‘j’ the component number within the sub-system. The main, wing and collector tanks in the fuel rig system each contain the same type of components, the only disparity being that the numbers in the codes start ‘01’, ‘02’ and ‘03’ for the respective tanks (‘04’ is also used to represent the ‘engine tank’).

4. Systems Modelling and Preparation Stage

4.1 Sub-System Identification/Sensor Locations

The fuel rig is divided into 4 ‘sub-systems’ as shown by the dashed lines in Figure 1. Three of the sub-systems contain the main, wing and collector tanks, and the fourth contains the refuelling part of the system, simulated using the engine tank.

The process variables that are monitored in each tank system are flow and level. The main, wing and collector tank sub-systems each possess a level transmitter within the tank itself, which is labelled LT0110 in Figure 2 for the main tank. There are also six flow transmitters; one after each of the powered isolation valves on L1 and L2 out of the tank (FT0110, FT0120), one where these lines join up on the main outflow line (FT0130), one on each of the overflow lines (FT0111, FT0121) and finally one on the drainage line (FT0100).

The key variables in the overall system are the level in the collector tank and the flow on the main outflow line of each of the three tanks. The level in both the main and wing tanks are also important factors to the system functionality as these could lead to the identification of a problem in an individual tank and potentially identifies hidden failures within the system.

4.2 System Operating Assumptions

A number of assumptions have been made regarding the function of the fuel rig system:

- A blockage in a pipe or valve will prevent any flow of fluid through this component. Similarly a partial blockage will reduce the amount of fluid flow in a pipe or through a valve, but not stop it completely.

- A fracture in a pipe will result in fluid leaving the system at this point, preventing any flow of fluid further into the system. A leak in a pipe or valve will cause partial flow and result in some loss of fluid from the system. All fluid losses cannot be replenished.

- A rupture in one of the tanks results in a loss of unwanted fluid out of the system that cannot be replenished. A rupture in the collector tank will lose fluid faster than it can be refilled from its supply, even if both main and wing tanks are being used.

- The system will always start off with the required level of fuel in the main, wing and collector tanks if the system is ACTIVE, DORMANT or FUEL DUMPING. If the system is in the REFUELLING mode the main, wing and collector tanks will be refuelled if the levels are below that required.

4.3 Patterns

The example in this paper will focus on the fuel rig system in the ACTIVE operating mode. Due to the complexity of the problem, the number of possible combinations of different patterns for all of the sensors is too large to deal with. To overcome this, in the case of being ACTIVE, the operating mode is split up into six 'sub-modes' that are dependent upon the level of water in the collector tank.

The readings from the level transmitters are: 'empty' (E), 'pump shut off' (PSO), 'low' (L), 'adequate section' (AS), 'required level' (RL), 'high' (H) and 'full' (F) as shown in Figure 3.

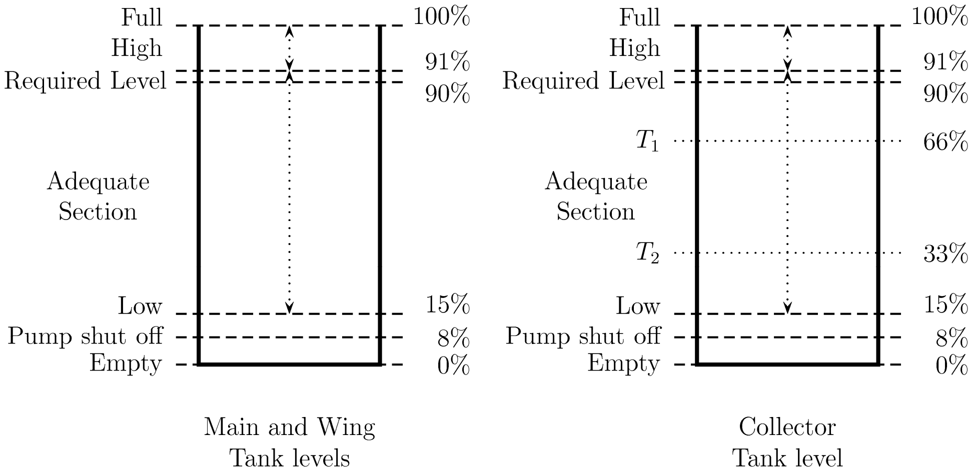


Figure 3. Tank levels for the fuel rig system.

The six sub-modes for the ACTIVE mode each results in a set of expected sensor readings for the key process variables if everything is working normally. The expected plots for the transmitters on the outflow lines of each of the tanks are shown in Table II (L_C indicates the level of water in the collector tank).

The key process variables (the flow transmitters in each tank and the level transmitter in the collector tank) in the system are monitored and expected plots from these are compared with actual patterns obtained in order to highlight any initial deviations.

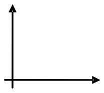
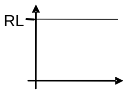
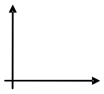
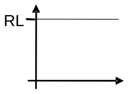
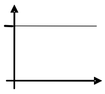
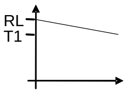
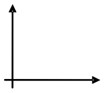
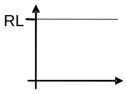
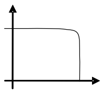
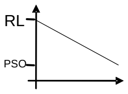
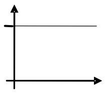
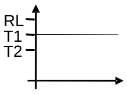
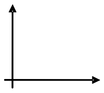
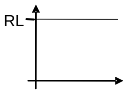
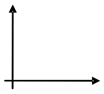
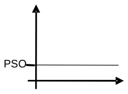
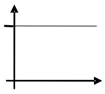
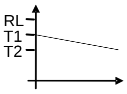
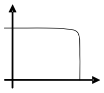
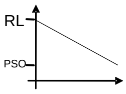
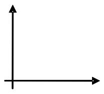
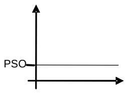
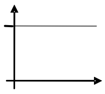
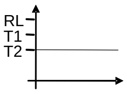
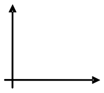
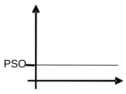
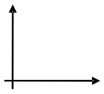
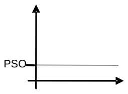
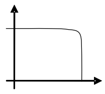
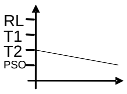
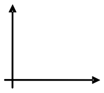
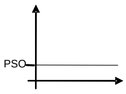
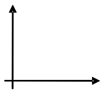
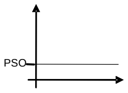
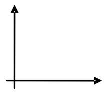
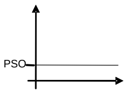
There are 3 possible conclusions for the patterns obtained from the system:

1. The readings for the key flow patterns and level pattern in the collector tank are as expected. The level of fluid in the tanks not currently delivering fluid is then checked for any indication of loss from the system.

2. There is inadequate flow out of a tank that should be providing flow at that specified point in the system.

3. There is a flow out of any of the three when tanks when there should not be flow.

Table II: Expected sensor patterns for outflow lines and levels in each tank.

	MAIN FT0130	**MAIN LEVEL** LT0110	**WING** FT0230	**WING LEVEL** LT0210	**COLLECTOR** FT0330	**COLLECTOR LEVEL** LT0310
ACTIVE1 ($T_1 < L_C \leq$ RL)						
ACTIVE2 ($L_C = T_1$)						
ACTIVE3 ($T_2 < L_C < T_1$)						
ACTIVE4 ($L_C = T_2$)						
ACTIVE5 (PSO < $L_C < T_2$)						
ACTIVE6 (L_C = PSO)						

Patterns deviating from those in Table II for each sub-mode are investigated and the regions in the system where a fault could potentially have occurred to cause this deviation are examined in more detail. For instance, when the system is in sub-mode ACTIVE1 the level in the collector tank should decrease, therefore any rise or no change in water level when flow is occurring out of the tank indicates a failure in the main or/and wing tank(s) . Any unwanted flow out of the main and wing tanks will also be signified at their key flow transmitters within these tanks. No flow out of the collector tank in sub-mode ACTIVE1 will be the result of a failure in that tank as the level of fluid initially starts at the required level.

Expected patterns within a sub-system for each operating mode are also established and investigated in the event of a deviation by a key transmitter. Expected patterns from sensors in the sub-system are compared to those actually obtained in the same way as for the main system. Any impossible combination of patterns for the sensors in a sub-system indicates a sensor failure.

4.4 Fault Tree Development

Non-coherent fault trees are drawn in order to determine the causality of deviations from expected sensor readings within the system. A tree is developed for each transmitter in a sub-system by taking into consideration the potential causes of failure within this part, thus restricting the boundary of causes to that particular section of the system.

Non-coherent fault trees are constructed for deviations from the expected observations for the flow transmitters on the drainage line and each of the streams L1 and L2. Due to the symmetry of the structure the potential causes of failure for each of these streams are the same, the only difference being the numbering on each line. When the transmitters are known to be functioning correctly this information is incorporated into the analysis by drawing a success tree. Fault trees are also drawn for the level transmitter in each sub-system, indicating a loss of containment within the tank itself or another part of the sub-system.

5. Fault Identification – Application Stage

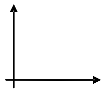
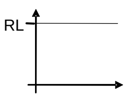
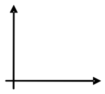
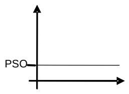
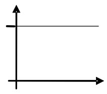
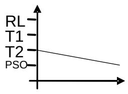
5.1 Identification of Sub-System Sensor Readings

The patterns in Table II are used to indicate a problem in the overall system function. No differences in the patterns from the key transmitters will indicate that the system is working as required. The levels in the non-supplying tanks are then checked to establish any fluid loss from the system.

Once a pattern deviation indicating unwanted flow/no flow out of a tank has been identified, the sub-system(s) on which a failure has occurred is identified. Patterns from the sensors within that/those section(s) are established and compared with expected results.

Assume for example there is no flow out of the main tank when it is required in sub-mode ACTIVE4. The system has been working as required up to this point. The actual readings obtained for the system are as shown in Table III.

Table III: Actual sensor patterns for the overall system in sub-mode ACTIVE4.

	MAIN	**MAIN LEVEL**	**WING**	**WING LEVEL**	**COLLECTOR**	**COLLECTOR LEVEL**
	FT0130	LT0110	FT0230	LT0210	FT0330	LT0310
ACTIVE4 ($L_C < T_2$)						

Citation: Hurdle, E.E., Bartlett, L.M. and Andrews, J.D., 2007. Fault tree based fault diagnostics methodology for an aircraft fuel system. IN: Proceedings of the 32nd ESREDA Seminar: Maintenance Modelling and Applications, 8-9th May, Hotel dei Pini, Località Le Bombarde – Alghero (SS).
This is a pre-publication version.

Key patterns not consistent those in Table II are FT0130 and LT0310. The pattern from the main tank level (LT0110) is also inconsistent as a result of no flow out of the tank. An unchangeable level in the tank indicates there is water present, unless the sensor has failed. Therefore there is at least one pattern not consistent with those expected in Table II for the given sub-mode, and the problem has been identified as being in the sub-system containing the main tank.

5.2 TOP Event Structure

A zero flow reading out of the main tank when flow is required indicates that both the working and redundant streams in that particular tank have failed. Each stream is looked at in turn along with post connection failures in order to ascertain the potential failure cause. Table IV shows an example of expected and actual sensor patterns for the working (L1) and redundant (L2) lines. It is assumed in this example that the recycle and stream flow transmitters are giving the same patterns for each stream. If there was flow out of the main tank as required then no flow would be expected along stream flow L2. The redundant line is used in the event of a failure causing no flow out of the sub-system as a result of a failure on L1 or on the post stream connection. Therefore the expected patterns for the system will also change, as shown in the second line Table IV.

Actual patterns from the system are indicating that both lines L1 and L2 have flow on the over flow lines but not out on the stream line. The flow sensor on the drain line is the only one giving the expected pattern for ACTIVE4. The expected patterns in the sub-system could indicate flow out on both streams. If this is the case then there must be a fracture failure either after each of the stream line flow sensors, or a failure after the two lines join.

Table IV: Expected and actual sensor patterns for the main tank sub-system when flow is expected on the outflow line.

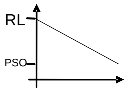
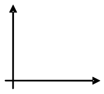
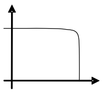
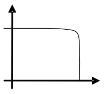
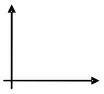
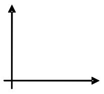
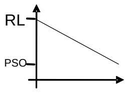
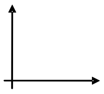
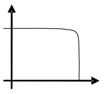
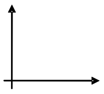
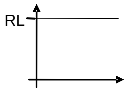
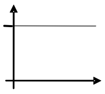
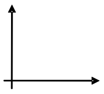
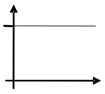
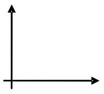
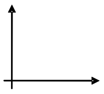
	LEVEL LT0110	**RECYCLE L1** FT0111	**STREAM FLOW L1** FT0110	**RECYCLE L2** FT0121	**STREAM FLOW L2** FT0120	**DRAIN FLOW** FT0100
ACTIVE4 Expected Patterns						
Operating Using Redundant Line		—	—			
Actual Patterns						

Figure 4 shows the causes of for the observed sub-system behaviour in a fault tree structure. The structure includes the causes of failure for zero flow at FT0130.

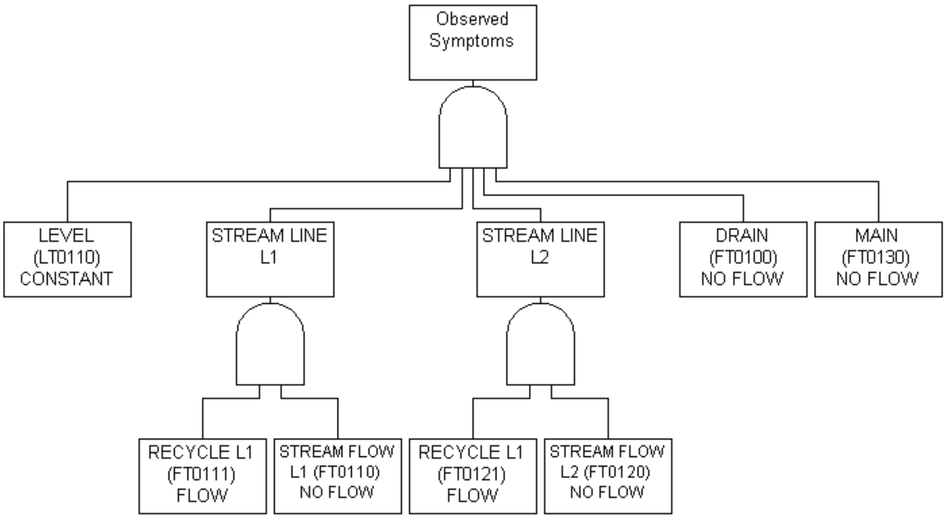


Figure 4. Causes of the observed sensor readings.

A qualitative analysis of this fault tree will produce a set of prime implicants that highlight the potential causes of failure for these given sub-system symptoms, along with the working components. Any working component states are then removed from the prime implicants by performing a coherent approximation, to give a list of potential causes of failure as shown in Table V.

Table V: Potential causes of failure.

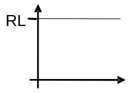
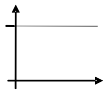
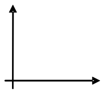
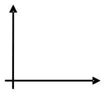
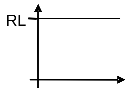
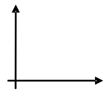
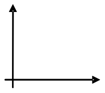
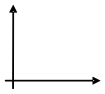
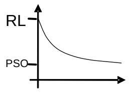
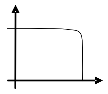
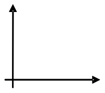
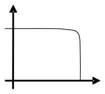
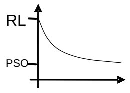
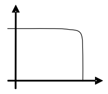
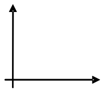
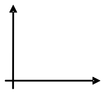
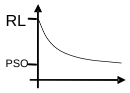
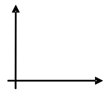
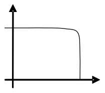
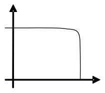
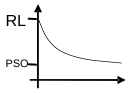
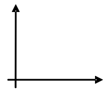
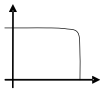
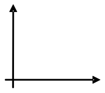
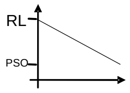
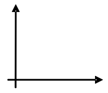
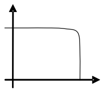
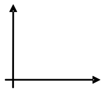
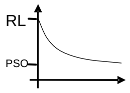
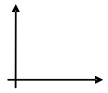
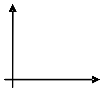
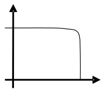
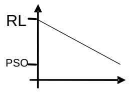
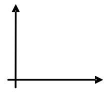
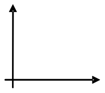
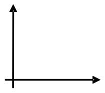
Where the Two Streams Meet	**OR**	**Failure on Stream L1**	**AND**	**Failure on Stream L2**
1) P0113B		1) P0103B		1) P0109B
2) P0114B		2) P0104B		2) P0110B
		3) P0105B		3) P0111B
		4) P0106B		4) P0112B
		5) BP0110B		5) BP0120B
		6) IVP0110FC		6) IVP0120FC
		7) IVP0110B		7) IVP0120B
		8) CT0110F		8) CT0120F
Potential Failure Causes: 2		Potential Failure Causes: 64		

There are 66 potential causes of system failure, 2 of order 1, as shown in the first column of the table and 64 of second order that are obtained by ANDing together the failures on stream L1 with those on L2. For instance, P0113B is a single failure and P0103B.IVP0120FC is a multiple failure containing two faults. Measures of importance [10] are used in order to identify the most likely cause of failure.

6. Results

Results have been obtained when the system is in sub-mode ACTIVE4 and the actual pattern of transmitter readings for key variables as shown in Table III, indicating a problem in the main tank section. The possible readings from the main tank sub-system are now looked at in more detail assuming that only high or no flow can occur at each flow transmitter in the section.

Table VI: Flow pattern results.

	LEVEL	**RECYCLE L1/L2**	**STREAM FLOW L1/L2**	**DRAIN FLOW**	**Results**		**Number of Actual Possibilities**
	LT0110	FT0111/FT0121	FT0110/FT0120	FT0100	n_i	nc_i	na_i
1)					66	66	66
2)					9	9	9
3)					132	132	132
4)					264	264	264
5)					10	10	10
6)					30	30	30
7)					5	5	5
8)					98	98	98
9)					9	9	321
Effectiveness Index I_E					0.892 (to 3 decimal places)		

Pattern combinations for the sensor readings are shown in Table VI. There are a number of combinations that are not present in the table as they cannot occur. For instance, any set of patterns containing a level that is not decreasing in the tank and the occurrence of flow on the drainage line (FT0100) or on either of the main outflow lines (FT0110 or FT0120) must be an invalid result. This indicates that there is a problem with a transmitter in the sub-system. The possible valid flow patterns for no or high flow are shown in Table VI. It is assumed that the flow patterns for L1 are the same for L2 in order to restrict the size of the problem to one that can be described in a short paper.

For each set of observed symptom Table VI contains the number of possible causes of failure identified by the method, n_i, the number of these that give correct causes, nc_i, and the actual number of potential causes that should be obtained, na_i.

The information obtained is used to calculate an Effectiveness Index I_E for the outcomes:

$$I_E = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{nc_i}{n_i}\right)\left(\frac{nc_i}{na_i}\right),$$

where, N is the number of level patterns investigated. The range of the index is from 0 to 1, where 0 indicates the method is completely ineffective and 1 showing that it is able to identify the correct failure for any set of observed symptoms.

In most cases the method has been able to correctly identify all potential causes of failure. In observed symptom 9) the method has only identified 9 potential failure causes, all of which are correct. Other failures that could cause this result include any blockage on line L1 in the system from pipe P0103 onwards and a fracture in either P0115 or P0116. A similar failure on line L2 would result in the potential causes of failure. These failures are masked by a normal no flow reading at FT0111 and FT0121.

The effectiveness index is I_E = 0.892, which indicates that the method works reasonably well at obtaining the potential failure causes in the system for a given set of symptoms.

7. Conclusions

The initial dynamic method developed for diagnosing faults in systems using fault tree analysis has been extended for use on a larger scale system containing redundancy. In most cases investigated the method has obtained the correct number of potential causes of failure for the system as shown for the sub-mode ACTIVE4. This is reflected in the Effectiveness Index. The method is not able to identify any hidden failures of components that have the same symptoms as when they are working as required. This is a difficulty in any method of analysis.

Breaking the system down into a set of sub-systems and dividing the operating modes into sub-modes dependent upon the level of water in the collector tank has reduced the complexity of the problem. Each sub-mode is inspected and any regions within the system in which a fault could have potentially occurred are examined in more detail. The work can now be tested on the actual fuel rig system.

Acknowledgements

The authors would like to thank BAE Systems for both information on the fuel rig system and financial support towards the research reported in this paper.

References

[1] Žužek A., Biasizzo A. and Novak F. (1996), "Towards a General Test Presentation in the Test Sequencing Problem", *Proceedings of the 2nd International On-Line Testing Workshop, IEEE Computer Society Press,* Biarritz, France, 236-237.

[2] Žužek A., Novak F., Biasizzo A., Savnik I. and Cestnik B. (1995), "Sequential Diagnosis Tool for System Maintenance and Repair", *Electrotechnical Review,* **62**:224-231.

[3] Biasizzo A., Žužek A. and Novak F. (2000), "Sequential Diagnosis Tool", *Microprocessors and Microsystems,* **24**:191-197.

[4] Biasizzo A., Žužek A. and Novak F. (1998), "Sequential Diagnosis with Asymmetrical Tests", *The Computer Journal*, **41** [3] 163-170.

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

[6] Hurdle E. E., Bartlett L. M. and Andrews J. D. (2005), "System Fault Diagnostics Using Fault Tree Analysis", *Proceedings of the 16th ARTS (Advances in Reliability Technology Symposium)*, 12th-14th April 2005, Loughborough University.

[7] Hurdle E. E., Bartlett L. M. and Andrews J. D. (2006), "Diagnosing Faults in Systems Using a Fault Tree Based Method", *Proceedings of the 4th Edinburgh Conference on Risk: Analysis, Assessment and Management*, 29th-31st March 2006, Edinburgh University.

[8] Hurdle E. E., Bartlett L. M and Andrews J. D., "Fault Tree Based Fault Diagnostics for Dynamic Systems", *Proceedings of the ESREL (European Safety and Reliability Conference)*, 25th-27th June 2007, University of Stavanger, Norway.

[9] Hurdle E. E., Bartlett L. M. and Andrews J. D. (2006), "System Fault Diagnostics Using Fault Tree Analysis", *Proceedings of the IMechE Part O, Journal of Risk and Reliability*, **221** [1] 43-55.

[10] Andrews J.D. and Moss T. R. (2002), "Reliability and Risk Assessment", Second Edition, Professional Engineering Publishing Limited, London and Bury St. Edmunds, UK.