Reliability Engineering and System Safety 94 (2009) 1107–1115

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

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

L.M. Bartlett *, E.E. Hurdle, E.M. Kelly

Aeronautical and Automotive Engineering Department, Loughborough University, Loughborough, UK

ARTICLE INFO

Article history:
Received 4 December 2008
Accepted 7 December 2008
Available online 30 January 2009

Keywords:
Fault diagnostics
Fault trees
Digraphs

ABSTRACT

With the growing intolerance to failures within systems, the issue of fault diagnosis has become ever prevalent. Information concerning these possible failures can help to minimise the disruption to the functionality of the system by allowing quick rectification. Traditional approaches to fault diagnosis within engineering systems have focused on sequential testing procedures and real-time mechanisms. Both methods have been predominantly limited to single fault causes. Latest approaches also consider the issue of multiple faults in reflection to the characteristics of modern day systems designed for high reliability. In addition, a diagnostic capability is required in real time and for changeable system functionality. This paper focuses on two approaches which have been developed to cater for the demands of diagnosis within current engineering systems, namely application of the fault tree analysis technique and the method of digraphs. Both use a comparative approach to consider differences between actual system behaviour and that expected. The procedural guidelines are discussed for each method, with an experimental aircraft fuel system used to test and demonstrate the features of the techniques. The effectiveness of the approaches is compared and their future potential highlighted.

1. Introduction

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

Early methods dealing with diagnostic capability focused on identifying faults at a specific point in time using a series of testing procedures [1,2]. A symptom–fault relationship is evaluated, where a series of tests are used to filter to the actual fault cause. These approaches have been found to be effective in identifying single faults and also work well as an offline evaluation mechanism, i.e. for systems which have a period of inactivity where testing can occur at appropriate times without disruption. This allows identification of any faults prior to operation. However, the characteristics associated with modern day systems require real-time diagnosis and to incorporate both adaptability and identification of multiple faults [3]. With systems and missions often involving changing conditions and operational modes, adaptability is key to perform diagnosis for the full mission or system life.

To accommodate these system characteristics extensions to the early testing procedures have been developed [4], in addition such tools as genetic algorithms [5] have been implemented, both with limited success. More recent approaches include using failure modes and effects analysis [6,7], fault tree analysis [8,9] and a combination of both [10]. The successfulness of these methods has been variable as the system complexity increases. The method of digraphs has been used for limited multiple failures [11] identifying the potential for real-time automated monitoring and diagnosis, with improvement needed in the number of faults revealed.

With a limitation on the number of effective real-time multiple fault diagnostic tools currently in the literature, this paper compares the most recent fault tree analysis and digraph-based approaches. The differences between [8] and [9] are that the best approach laid out in these papers is extended to a larger system and the work considers system dynamics using flow pattern recognition. The approach can still obtain multiple failures and checks for consistency. With regard to reference [11], this paper considers process variables not just component failure modes, and also process variable effects are considered. Reference [11] uses a more prognosis-based approach for identifying weak links whereas this research using the method of back-tracing. The evaluation of both methods is based on the application to an aircraft fuel rig system. The methods include the capability to

* Corresponding author. Tel.: +44 1509 227276; fax: +44 1509 227275.
E-mail address: L.M.Bartlett@lboro.ac.uk (L.M. Bartlett).

0951-8320/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.12.005

evaluate multiple fault causes from a given system deviating state, inclusion of transient effects and analysis of dynamic system behaviour is considered, and both are adapted to include a form of consistency check for the results obtained. The work has the added originality of being applied to an experimental simulator which aids the validation of the results.

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

2. The diagnostic methods

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

2.1. Fault tree diagnostic method

Fault tree analysis has been around as a reliability assessment technique since the 1970s. It is concerned with the analysis of failures and provides a diagrammatic description of the various causes of a specified system failure in terms of the failure of its components [12]. Utilising the method for fault diagnostics involves the following steps:

Step 1 – *component and sensor identification*: Identify the components contained within the system and the failure modes of each. Identify the sensors contained or needed within the system to be used to monitor system behaviour.

Step 2 – construct fault trees for observable system deviations: The behaviour of the system can be monitored by sensors located at specific points, i.e. flow meters. Fault trees are constructed to represent the failure modes at these locations, i.e. high flow. Non-coherent fault trees are constructed that include failure and success states of the components, which removes inconsistencies between working and failed components. An example is given in Fig. 1 to represent unwanted high flow at a valve (valve 1, shown in Fig. 2). Using not logic one cause is because the valve has failed open, and hence it cannot fail closed. The valve has an inlet pipe and an outlet pipe (pipes 1 and 2), in order for flow to occur water must be available from the main supply and able to pass through the pipes. The necessary success events have been included in the right-hand branch.

Step 3 – determination of system status: Compare the readings indicative of the current system behaviour with those that are expected given the mode of operation. Deviations are representative of faults present.

Step 4 – *diagnostic fault tree construction*: Construct a top event structure from the sensor deviations identified in step 2. Combine all readings using an AND gate if there are more than one. Perform a standard qualitative analysis to obtain potential causes of failure.

Step 5 – *consistency verification*: Check the potential causes of system failure obtained in step 3 against the sensors reading true to the operating mode. Any potential causes of failure that could cause these true sensor readings to be false can be removed.

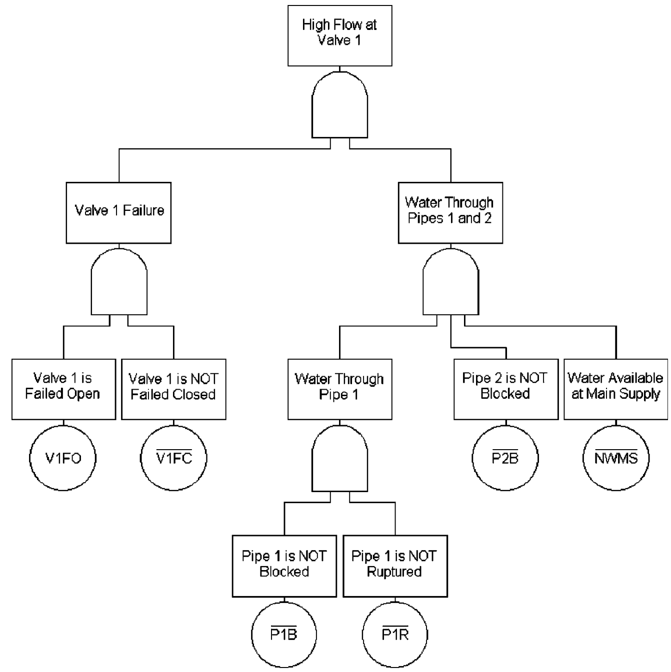

Fig. 1. Example non-coherent fault tree.

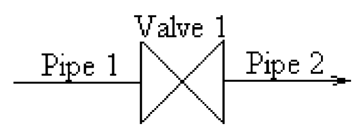

Fig. 2. Valve example.

Step 6 – fault cause ranking: In the instance of multiple fault cause options importance rankings can be used to determine the most likely cause of failure.

2.2. Digraph diagnostic method

Digraphs [13] can be used within engineering applications to represent the interrelationships between the process variables, such as temperature, mass flow and pressure. A diagram is constructed where nodes (or circles) are used to represent the process variables and edges (lines) are used to represent the interconnections, i.e. positive/negative influences. Nodes also represent component failure modes, whereby a signed edge connecting a failure mode node to a process variable node indicates the disturbance which the failure mode can cause. A simple digraph representation of a valve system unit (Fig. 2) is illustrated in Fig. 3. The valve unit is comprised from three components; namely, pipe 1, pipe 2 and valve 1.

The respective valve unit digraph depiction is formed by taking the process variable mass flow into consideration. The nodes M1 and M2 represent mass flow at pipes 1 and 2, respectively. The relationship between the two nodes is reflected by the three edges. M1 is the independent variable while M2 is the dependent variable since a directed edge connects M2 to M1. The edge with a gain of +1 is a normal edge since this represents the relationship which is usually true. For the valve unit case, this symbolises the fact that under normal circumstances mass flow in pipe 1 has a positive effect on mass flow in pipe 2 (i.e. valve open). The second and third edges are conditional edges since their relationship is