INTERRELATION RELIABILITY ANALYSIS OF FAULT TOLERANT FLIGHT CONTROL SYSTEM

Wang Shaoping
Department of Automatic Control,
Beijing University of Aeronautics and Astronautics,
Beijing 100083, P. R. China

Abstract

Modern Fault-tolerant Flight Control Systems (FFCS) are mostly composed of hardware and software which performance is affected by their interrelation such as function, running, failure and maintenance. Therefore, when analyzing the system's reliability, the influence of their interaction must be considered. In this paper, we study on the interrelation reliability analysis of the fault-tolerant flight control system with combination of FMECA and FTA. This method is partly based on the knowledge database, that is, some of the FMECA information comes from the knowledge database, and the other comes from the analyzers. When the FMECA information of the system is enough, the subtrees of the system's typical components can be constructed with the aid of the computer, and that will help the analyzers finish the construction of the system's entire fault tree.

1 Interrelation Failure Mode Analysis of Fault-Tolerant Flight Control System

Usually, FFCS adopts fault-tolerant software and hardware redundancy in order to obtain high reliability and safety. Its common failure mode includes software failure, hardware failure and the interface failure. According to statistics data, it is often obtain the independent software failure data and independent hardware failure data in initial development of computer system. But it is found that there also exist many failures in synthetic test after independent software failure and hardware failures have been corrected. It is obviously that the interrelation failures between software failures and hardware failures play an important role in FFCS, which are originated from the imperfect requirement, imperfect distribution and error. So the interrelation failures must be considered in Reliability analysis.

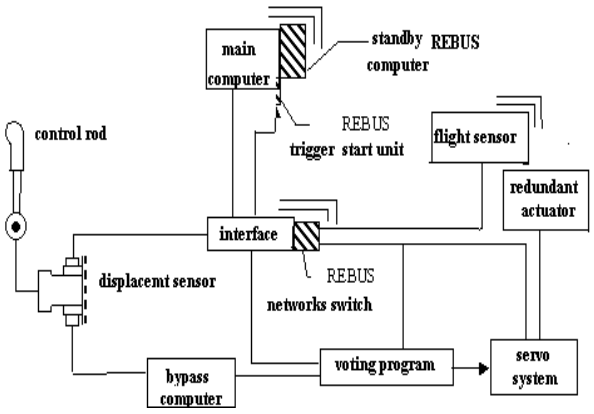

Fig1 A fault-tolerant flight control system

Fig1 shows a typical FFCS, which is composed by three redundant main computers, three redundant bypass computers, three redundant software, three standby software, one displacement sensor and one redundant actuator. When the main software of every channel fails, the standby software will be switched on. To every channel, the system fails if hardware failure and bypass computer failure, both main software failure and standby failures, displacement sensor failure and redundant actuator failure.

The main software of every channel could recover from transient failure by carrying it continuously to ensure system safety. If the program exists the failure, it can be cancelled by voting equipment. Every standby software can be triggered to switch on by voting program of interface network.

From analysis aforementioned, the interrelation failure mode are

- displacement sensor failure;
- redundant actuator failure;
- Independent main computer failure;
- Interface failures;
- Independent bypass computer failure;
- Independent software failure;
- Independent standby software failure;
- Voting equipment failure
- Interrelation failure of main computer;
- Interrelation failure of bypass computer.

Here the interrelation failure expresses the condition that lead to more than one channel (version to software) fail because of common failure cause.

2 Combination Reliability Analysis of FMECA and FTA

FMECA and FTA are two kinds of typical methods used for analyzing causality of the system's failure. By analyzing the potential failure's cause of every component in the system, FMECA can be used to find the failure mode with high criticality level, and present the effective measures to mend the system. Usually FMECA procedure starts with the system's lowest level such as component, and analyzes each level bottom-up until the indenture level such as system. In FTA, a top event (specific undesirable system's state or failure) is defined. The procedure use the detective reasoning top-down to find the causes leading to the top event's occurrence, until the basic events are found.

FMECA and FTA are two kinds of simple analysis technique, which don't refer to profound theory. Their analysis results are useful for improving the system's reliability, so they are used widely in practical project. While analyzing the complex system, they are limited for their tremendous workload. On the other hand, both FMECA and FTA have their disadvantages. For example, FMECA isn't very direct for the description of system's reliability and safety and its capacity for quantitative analysis isn't powerful, while FTA can not demonstrate the system's reliability information as comprehensively as FMECA. Therefore how to reduce FMECA and FTA's workload and utilize their advantages are the main problems to be solved. In addition, how to use FMECA and FTA to analyze the reliability of hardware and software synthetic system is the another question worth being researched. This paper presents the computer-aided combination technique of FMECA and FTA to solve the problems aforementioned.

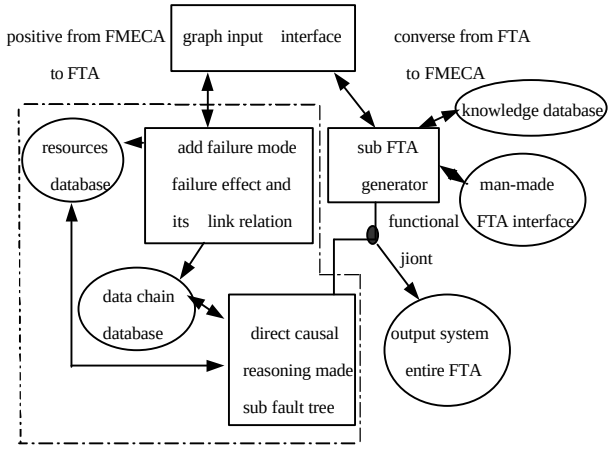

Fig 2 Combination analysis of FMECA and FTA

2.1 The Positive Reasoning from FMECA to FTA

Fig2 is the basic theory of combination reliability analysis. It is obviously that this method absorbs the advantages of FMECA and FTA and saves the analysis workload greatly with the aid of computer.

The combination of FMECA and FTA takes its source at inference way. Cause and effect reasoning technique adopts the inference model to replace the reasoning rule and software, that is using the FMECA tabular and its cause-effect reasoning relation between lower lever and topper to inference the sub fault tree automatically. The direct causal reasoning way is described in Fig3.

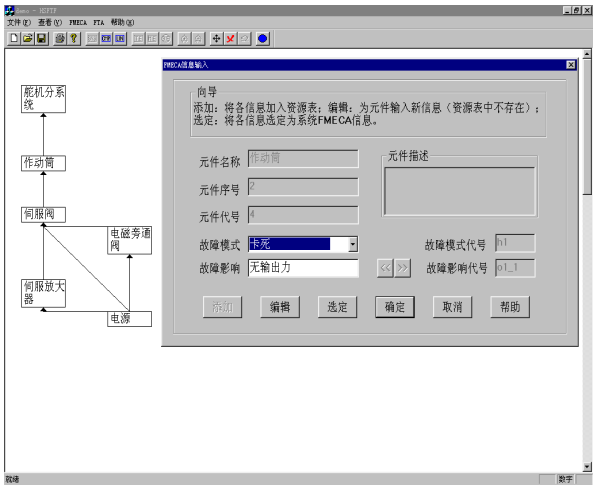

Fig 3 The direct causal reasoning method

If a part of unit is not related to other part in fault-tolerant control system, it is easy to establish the sub fault tree with direct causal reasoning. Fig 4 shows the direct causal reasoning diagram of redundant actuator through the user's graph input interface, where every block expresses one component and every link line expresses the cause and effect relation (the relation is stored in data chain database).

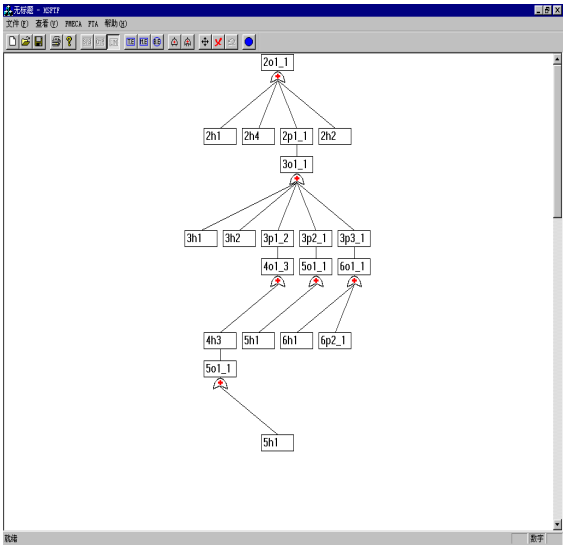

Fig 4 The sub fault tree of redundant actuator

Click one block, the FMECA tabular and data chain relation tabular will arise, then the sub fault tree can be obtained after determining the corresponding failure mode and failure effect. So the theory of direct causal reasoning method is to inference the sub fault tree from the data source data base and data chain database. This method is called a positive reasoning from FMECA to sub FTA.

2.2 The Converse Reasoning from FTA to FMECA

From Fig 1, it indicates that the computer system fails if the following condition appears.

(1) Two of three main system fail;

(2) The main software fails and the standby software is switched on;

(3) The bypass imitate computer is switched on through unit interface after main computer having failed.

(4) In bypass computer, all of them fail.

Considering the failure mode interrelation and the dynamic performance degradation, the dynamic FTA of computer system described in Fig 1is showed in Fig5.

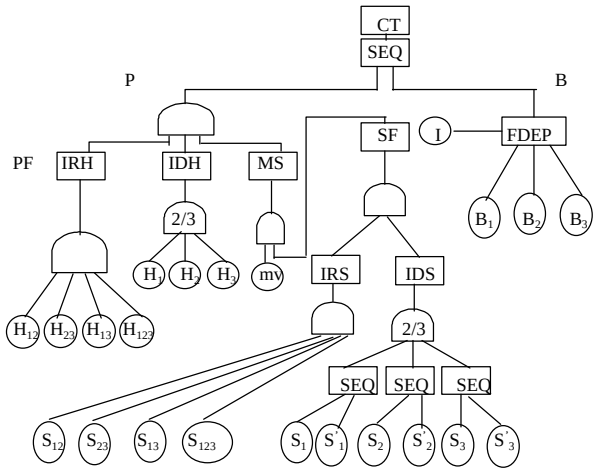

Fig 5 The converse reasoning method

Where CT—computer failure;

P—failure of the main computer;

PF—the failure of main hardware;

IRH—independent failure of hardware;

IDH—interrelation failure of hardware;

SF—the failure of main software;

IRS—independent software failures;

IDS—interrelation failure of software;

S_1, S_2, S_3 —main software failure of three channels respectively;

H_1, H_2, H_3 —main hardware failure of three channels respectively;

$S_1^{'}, S_2^{'}, S_3^{'}$ —standby software failure of three channels respectively;

mv— the voting program failure;
MS—the software part failure;
I—the unit interface failure;
B_1, B_2, B_3—bypass computer failure of three channels respectively;
B—bypass computer system failure;
S_{xyz}—software failures of channel x, y and z because of a common cause (x, y, z∈ 1,2,3);
H_{xyz}—hardware failures of channel x, y and z because of a common cause (x, y, z∈ 1,2,3);
SEQ—the sequence gate;
FDEP—the functional dependency gate.

Fig 5 is obtained by converse reasoning from FTA to FMECA. Analyzer uses the graphic tool, which include dynamic gates and event block, to establish the computer FTA. On the graphic of sub FTA, click the component, user can search and add the failure mode, its immediate or ultimate influence and its criticality.

2.3 Combination Reliability Analysis between FMECA and FTA

To complex FFCS system, FMECA can easily analyze the cause and effect relation, FTA can consider failure influence of multi-factors, interrelation and dynamic procedures. So combining the positive reasoning and converse reasoning to form a combination reliability analysis method is content to FFCS. Generally, the whole FFCS can be divided into two parts by functional joint: one part that is located before function joint and one part is located after function joint. The first part uses the positive reasoning from FMECA to FTA to establish the sub fault tree, and the second part applies the converse reasoning from FTA to FMECA to represent the dynamic procedure. Combine the two types of sub fault tree to obtain the entire FTA of FFCS.

3 Conclusion

Because the fault-tolerant control system is composed by hardware and software, which is a complex dynamic system and has interrelation of function, running, failure and maintenance, so the historical method of assuming the hardware and software are independence is inappropriate. This paper analyses the interrelation and dynamic procedure of fault-tolerant flight control system and presents the reliability analysis on FFCS with the combination approach of FMECA and FTA. It can be used in other fault-tolerant system with hardware and software. The key is how to select the functional joint, how to construct the reasonable component information database, how to simplify the reasoning process and how to make the combination of FMECA and FTA perfectly. The application of FFCS indicates that this method can not only save the reasoning time and workload greatly, but also can solve the dynamic interrelation problem. So the combination reliability method between FMECA and FTA is satisfied to fault-tolerant control system.

Reference

[1] Zhou haijing, the application of the simulating software in FMEA, Proceedings of The fourth International Conference on RELIABILITY, MAINTAINABILITY AND SAFETY, pp219~223, May 1999.

[2] David J. Russomanno, Ronald D. Bonnell, John B. Bowles, Functional Reasoning in a Failure Modes and Effects Analysis (FMEA) Expert System, 1993 Proceeding Annual Reliability and Maintainability Symposium, pp339~346.

[3] Daniel Bell, Lisa Cox, Steve Jackson, Phil Schaefer, Using Causal Reasoning for Automatic Failure Modes & Effects Analysis (FMEA), 1992 Proceeding Annual Reliability and Maintainability Symposium, pp343~353.

[4] Fred M. Hall, Raymond A. Paul, Wendy E. Snow, Hardware/Software FMEA, 1992 Proceeding Annual Reliability and Maintainability Symposium, pp320~327.

[5] Jian Zhimin, A New Approach To Constructing The Fault Tree of The Control System, Dissertation for Doctor Degree from TSINGHUA University, 1993.