FDIR and Integrated Evaluation For Fault-Tolerant Elevator System

Jin Zhang[1, a] , Qifu Fan[1, b]

[1]Automation Department of Shanghai Jiao Tong University, Shanghai, 200240, China;

[a]zhangjin123@sjtu.edu.cn, [b]qffan@sjtu.edu.cn

Keywords: FDIR, fault-tolerant system, fault-tolerant management, reliability evaluation

Abstract. This paper presents a fault detection, isolation and reconstruction (FDIR) mechanism for the fault-tolerant system. A self-detection component is introduced to the normal dual-channel redundant system, and the component can detect the outputs of the behavior model and the nominal system model. The control strategy is reconfigured by using the differences between the outputs of the behavior model and nominal model so as to improve the reliability and performance requirements of the system. The fault-tolerant management mechanism considers the metrics of the reliability of the elevator system and the performance requirements. Based on the evaluation tool developed on Matlab/Simulink, we assess the case of the elevator fault-tolerant system with the self-detection component and verify the effectiveness of this methodology.

Introduction

The task of flight control system is to control the aircraft. In modern civil aircrafts, fly-by-wire flight control system(FBW FCS) is normally used. As a key subsystem concerned with flight safety, it plays an important role, and its structure is becoming more and more complicated. Therefore, reliability and safety have become critical issues in the design process of flight control system. At present, some foreign famous Aircraft manufacturers, such as Boeing and Airbus, all have their own reliability management schemes. The FDIR redundancy management algorithm discussed in this paper is developed for ARJ21 aircraft.

Fault tolerant flight control system can significantly improve the reliability of the aircraft, and can still maintain the aircraft performance in the event of component failures[1]. To improve the reliability and fault tolerance of flight control computer, the best way is taking measures from the system, which is referred to redundancy technique[2].

Model establishment and FDIR

To a dual-channel elevator system, the paper presents a fault tolerant control strategy with fault detection, isolation and reconfiguration (FDIR), that is, by the introduction of a self-detection device, which can detect the difference between system behavior model output and nominal model output, and use the deviation to determine reconfiguration strategies of control law . The reliability and performance metrics and associated requirements of the elevator system are considered in the fault tolerance management scheme. Then, based on MATLAB / Simulink tools, we assess the reliability and performance of the improved dual-channel elevator system with self-detection device , which verifies the effectiveness of the proposed fault-tolerant control strategy.

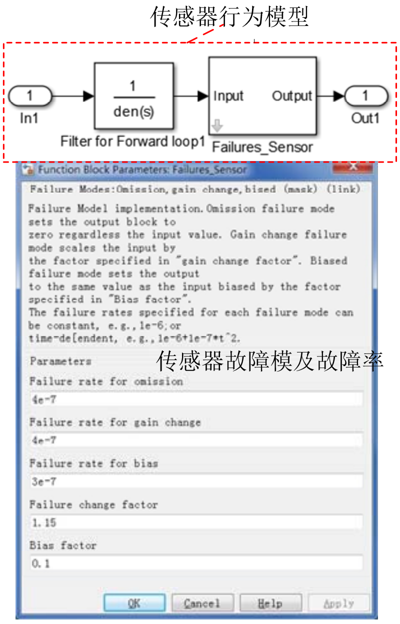
Nominal model definition. The nominal model is the system model under the condition that no fault occurs in any subsystem[3].The first step of the reliability analysis based on the model is to create a standard description of the system. The behavior of a system can be described by some language that supports graphics or text, such as Lustre language[4] which supports text and the graphical tool SCADE[5] . In this paper, we use the graphical tool Simulink to model the nominal behavior of the system.

Component failure model definition. A failure is the event that a system or component can not complete a specified function due to some causes that cause the deviation from the normal operating state. The failure mode is the concrete manifestation of failure.

Taking the position sensor in the actuation system of the elevator control system as an example, the sensor has 4 failure modes[6][7].

$$\hat{y}_{sr}=\begin{cases} y_{sr}, & U_f=0(failure\_free\_N) \\ 0, & U_f=1(omission\_O) \\ Gy_{sr}, & U_f=2(gain\_change\_G) \\ y_{sr}+B, & U_f=3(baised\_B) \end{cases}$$

System behavior model. The system behavior model is obtained by injecting the failure model of the various components into the nominal model of the system. Take the elevator position sensor as an example, the behavior model is shown in Figure 1.



Failure Modes:Omission,gain change,bised (mask) (link)

Failure Model implementation.Omission failure mode sets the output block to zero regardless the input value. Gain change failure mode scales the input by the factor specified in "gain change factor". Biased failure mode sets the output to the same value as the input biased by the factor specified in "Bias factor".
The failure rates specified for each failure mode can be constant, e.g.,1e-6;or time-de[endent, e.g.,1e-6+1e-7*t^2.

Parameters

Failure rate for omission
4e-7

Failure rate for gain change
4e-7

Failure rate for bias
3e-7

Failure change factor
1.15

Bias factor
0.1

Fig.1 Behavior model of sensor

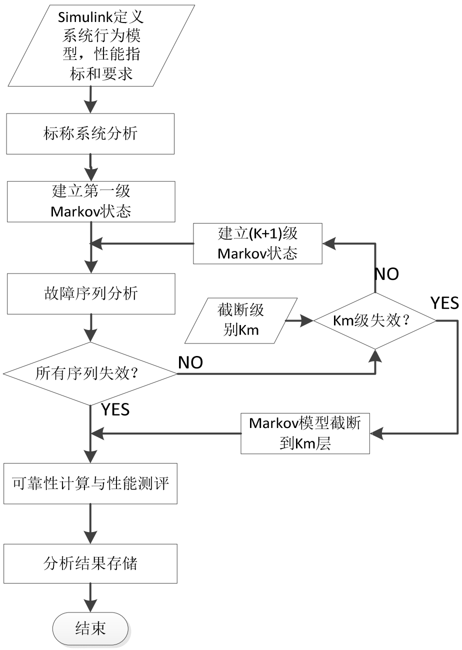


Fig.2 Program diagram of evaluation tool

Failure detection, isolation and reconfiguration mechanism. In this paper, we use model-based design with Matlab/Simuilink to design a FDIR mechanism for the ordinary dual-channel elevator system.

FDIR mechanism

1.Failure detection : The self-detection circuit implemented in each ACE checks the range of the output signals of the PCU, and compares it with the nominal output. If the difference between the actual output and the nominal output is within a certain range, then the system is considered normal, otherwise the self-detection circuit reports a failure. Additionally, the rate of change of the outputted signals is checked, and if the self-detection circuit detects no rate of change, then a failure is reported.

2.Isolation : Once the self-detection circuit reports a failure, the main ACE is shut down.

3.Reconfiguration : Once the self-detection circuit detects a failure, a reconfiguration signal is sent to the remaining ACE to change the gain of the control surface actuation subsystems controller. The reconfiguration strategy should compensate for the fact only the control surface actuation subsystems commanded by the remaining ACE are operational.

Simulation and case study

Based on the integrated evaluation tool developed on Matlab/Simulink, the ordinary dual-channel architecture and the improved dual-channel architecture with FDIR mechanism are evaluated. The evaluation flow chart is shown in Figure 2.

Model definition of the elevator system. The schematic diagram of the elevator system is shown in Figure 3, which consists of the primary actuator control electronics (P-ACE), actuator (PCU), elevator control surface and structural support units. P-ACE receives the elevator position signal from the flight control computer (FCC), and compares the position signal with the actual position signal of the PCU. Then the error signal is converted into the current control signal to the electro-hydraulic servo valve. The current signal changes the opening degree of the main valve spool so the actuator cylinder can drive the control surface to the command position.

The position signal of the actuator cylinder is detected by the linear variable differential transducer (LVDT) and transformed into electrical signal sent to P-ACE.

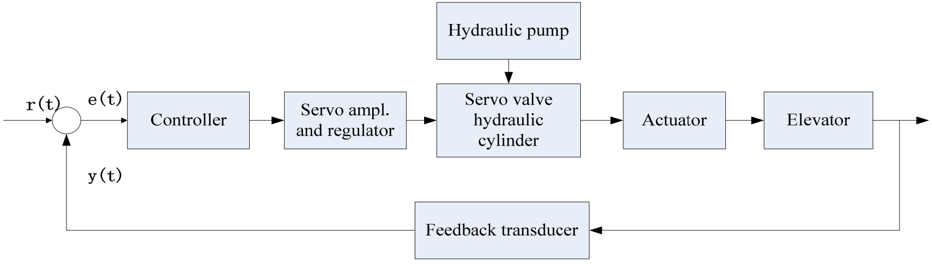


Fig.3 Schematic of the section of elevator system

Component failure model. Table 1 collects the information corresponding to the failure models of the different hardware component in the elevator system[8]. The possible failure modes of each component are listed in column 2, while column 3 is an explanation of the effect of each failure mode on the component behavior. U_f in column 4 is the variable the assigns the corresponding failure mode to the component behavior model equations. The last column of the table λ collects the failure rates associated with each failure mode, which are necessary to build the state-transition matrix associated with the Markov reliability model. The simulation model of the elevator system is shown in Figure 4.

Table 1 Component failure model parameters

Component	Failure mode	Description	U_f	Failure rate
P-ACE	Omission	Outpt set to zero	1	$2x10^{-7}$
	Random	Random output between -0.5 and 0.5	2	10^{-7}
	Delayed	Output delayed 2s	3	10^{-7}
PCU	Omission	Outpt set to zero	1	10^{-6}
Surface	Omission	Outpt set to zero	1	10^{-8}
Sensor	Omission	Outpt set to zero	1	$4x10^{-7}$
	Gain-change	Output scaled by a factor of 1.15	2	$3x10^{-7}$
	Biased	Output biased by a factor of 0.1	3	$3x10^{-7}$

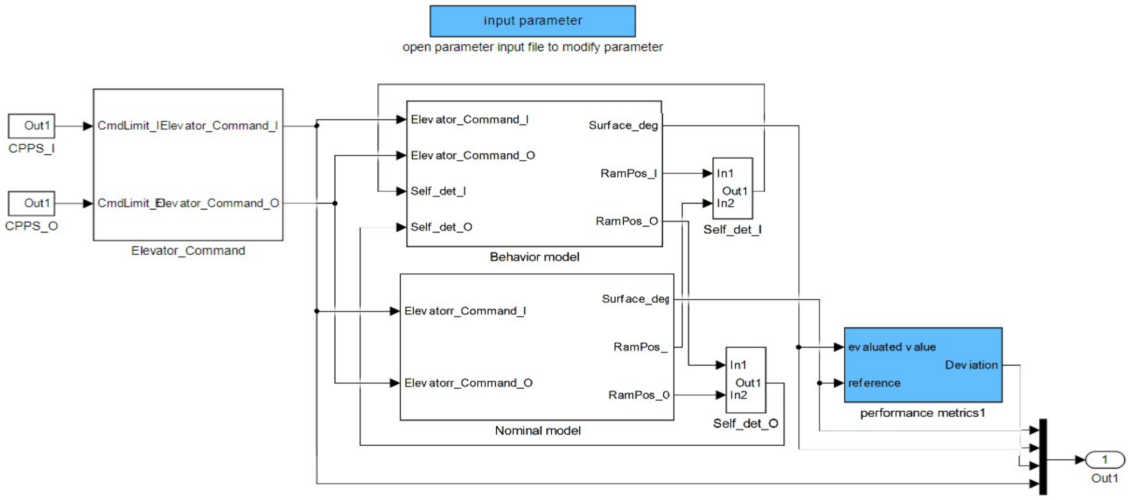


Fig.4 Simulation model of the elevator system

Performance metrics definition and associated requirements of the elevator system. For the elevator system under consideration， the design goals are threefold:

1.The system must tolerate any single component failure, i.e, it must be single fault-tolerant.

2.The system must be able to operate without any maintenance for 0.5h.

3.The system failure rate $\lambda(t)$ must not exceed 10^{-6} failures/hour.

From (2) and (3), the unreliability Q of the elevator system under consideration at the end of the maintenance period must not exceed 2×10^{-7} .i.e.$Q\le 2\times10^{-7}$.

System evaluation and results analysis. The system evaluation is carried out under specific conditions. The aircraft time constants dictate a configuration evaluation time $t_c = 20s$ .So in this case, a 5 rad.0.1Hz square wave in the elevator command is chosen. And the fault injection time t_f is set to $2s$. Therefore, in the remainder of the evaluation time (18s), if the difference between the actual system output and nominal model output conform to the performance requirements, it is determined that the new system configuration is normal; and if the deviation don't conform to the performance requirements, it is determined that the new configuration failed. The system global evaluation time *T* is set to 0.5h. The reference elevator dynamic response is shown in Fig.5 together with the elevator command.

Fig.6-9 show the dynamic response of the behavior model when the component failures are injected. Fig.6 shows the elevator response for a single failure in the PCU. Fig.7 shows ACE random failure. Fig.8 shows ACE delayed failure. Fig.9 shows sensor output omission failure. Figure a) shows the dynamic response of the dual-channel architecture. Figure b) shows the dynamic response of the improved dual-channel architecture which is added FDIR mechanism.

Table 2 Evaluation results of ordinary dual-channel architecture

Component failure mode	Failure rate	Index	State probability	System state	Maximum deviation
No Failures		1	0.9999	1	0
Surface/omission	1E-08	2	2E-09	0	4.9811
PCU_I/omission	1E-06	3	2E-07	0	3.1291
ACE_I/omission	2E-07	4	4E-08	0	7.0585
ACE_I/random	1E-07	5	2E-08	0	4.5814
ACE_I/delayed	1E-07	6	2E-08	0	11.7487
Sen_I/omission	4E-07	7	8E-08	0	2.7889
Sen_I/gainchange	4E-07	8	8E-08	0	0.5341
Sen_I/biased	3E-07	9	6E-08	0	11.7548

Table 3 Evaluation results of improved dual-channel architecture

Component failure mode	Failure rate	Index	State probability	System state	Maximum deviation
No Failures		1	0.9999	1	0
Surface/omission	1E-08	2	2E-09	0	4.902201
PCU_I/omission	1E-06	3	2E-07	1	0.123419
ACE_I/omission	2E-07	4	4E-08	1	0.287942
ACE_I/random	1E-07	5	2E-08	1	0.278208
ACE_I/delayed	1E-07	6	2E-08	1	0.278033
Sen_I/omission	4E-07	7	8E-08	1	0.27817
Sen_I/gainchange	4E-07	8	8E-08	1	0.270868
Sen_I/biased	3E-07	9	6E-08	1	0.278216

Tables 2 and 3, respectively, show the evaluation results of the ordinary dual-channel architecture and the improved dual-channel architecture, where state status 1 represents the system is normal and 0 indicates the system failed.

Figure 6(a) shows the dynamic response of the ordinary dual-channel architecture when PCU output omission failure is injected. It can be seen that 2s after the failure occurs, the deviation between the actual system output and nominal model output is far less than the performance requirements. In this case, the failure is catastrophic. Figure 6(b) shows the dynamic response of the improved dual-channel architecture. By improving the fault tolerant technique with FDIR mechanism, the difference between actual output and nominal output is less than 0.3, far lower than the original deviation which was 4.58. The results show that, the elevator still response the position command rapidly and accurately, when sensor, PCU and ACE are injected with failures.

Table 4 shows the evaluation results of the unreliability in the ordinary dual-channel architecture and the improved dual-channel architecture. It can be seen that, by introducing FDIR mechanism to the ordinary dual-channel system, the system unreliability decreases, so the system reliability is improved.

Table 4 Unreliability comparison of two kinds of fault tolerance architectures

Fault tolerant structure	Unreliability
Ordinary dual-channel architecture	1.002E-06
Improved dual-channel architecture with FDIR mechanism	2E-09

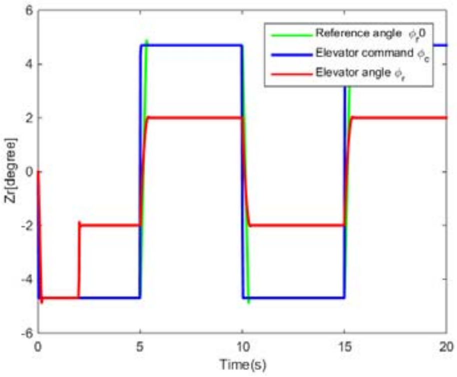


Fig.6(a) Omission failure of PCU

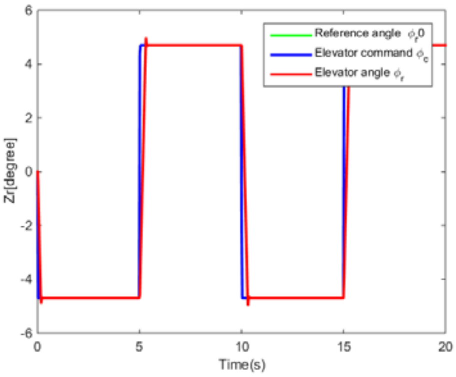


Fig.6(b) Omission failure of PCU

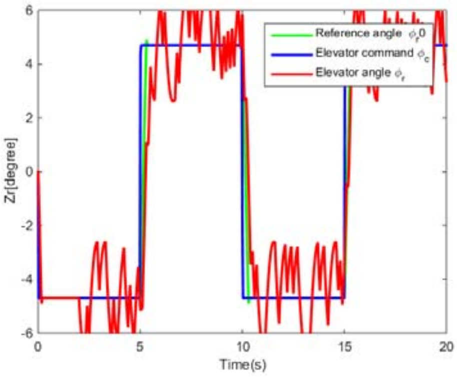


Fig.7(a) Random output failure of ACE

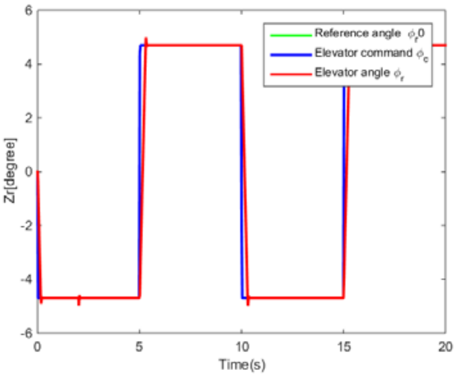


Fig.7(b) Random output failure of ACE

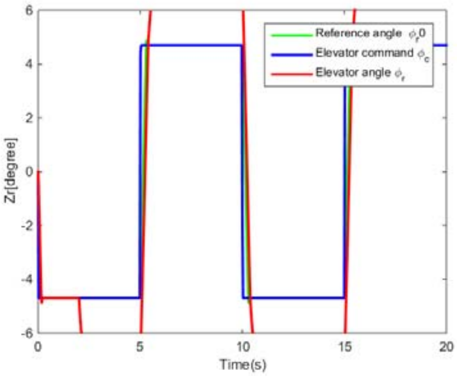


Fig.8(a) Omission failure of sensor

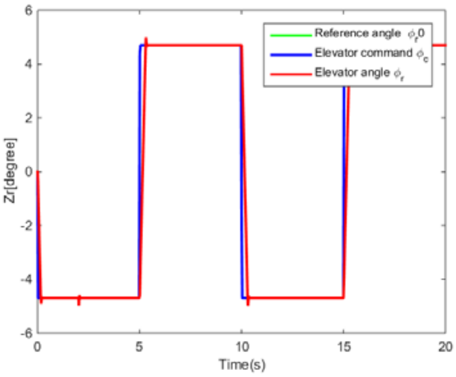


Fig.8(b) Omission failure of sensor

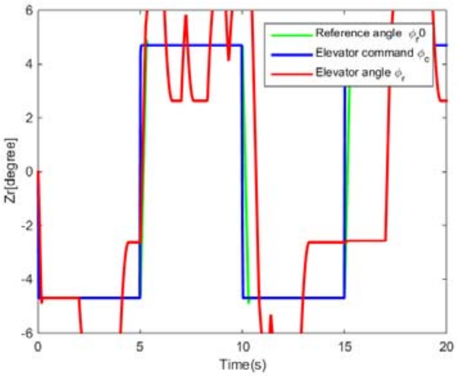


Fig.9(a) Delay failure of ACE

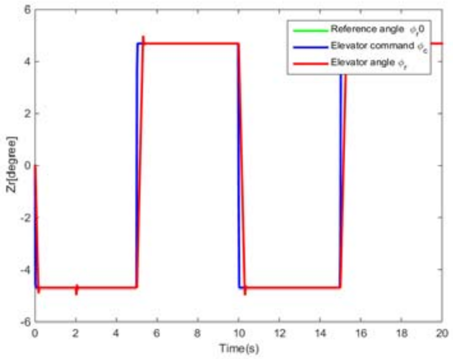


Fig.9(b) Delay failure of ACE

Conclusion

In this paper, a behavior model for the ordinary dual-channel elevator system is built based on Matlab/Simuilink, and its reliability and performance are assessed using the integrated evaluation tool developed on Matlab. According to the weak points identified from evaluation in the elevator system, an improved method is proposed by introducing FDIR device based on the original dual-channel architecture, and also assess its reliability and performance. Finally, the results show that the proposed method can significantly improve the reliability and performance of the elevator system, and eliminate single points of failure greatly in the elevator system.

References

[1] Weiguo Zhang, Xiaoxiong Liu, Wenguang Li,et al, Fault Isolation and Adaptive Reconfiguration Design for Fault Tolerance Flight Control System[J]. Journal of North University of China (Natural Science Edition), 04 (2007) 304-309.

[2] Xiaoxiong Liu, Huaimin Chen, Weiguo Zhang, Chengfu Wu, Yijun Huang, Design of Self-Monitoring Dual Redundancy Flight Control Computer Systems[J]// Measurement & Control Technology,07 (2005) 72-75.

[3] A D Dominguez-Garcia, J G Kassakian, J E Schindall, et al, On the Use of Behavioral Models for the Integrated Performance and Reliability Evaluation of Fault-Tolerant Avionics Systems[C]// 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA. IEEE, (2006) 1-14.

[4] N Halbwachs, P Caspi, P Raymond, et al, The synchronous dataflow programming language LUSTRE[J]. Proceedings of the IEEE,79(9) (2000) 1305-1320.

[5] A Joshi, M P E Heimdahl, Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier.[M]// Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, (2005) 122-135.

[6] Wei Yang,et al, Fault tolerant flight control system[M] Northwestern Polytechnical University Press, (2007):30-35.

[7] Anhong Qin, Automatic integrated evaluation for the performance and reliability of rudder system[D]. Shanghai Jiao Tong University, (2014).

[8] Jing Wang, Fault diagnosis technology research and software development of the flight control system[D]. Northwestern Polytechnical University, (2007).