Safety design method of a civil aircraft cargo door actuation system

Wang Danyang1, Xu Haobang1, Wang Xiaolu1, Wu Hao1, Nie Zhenjin1
1Beijing Institute of Precision Mechatronics and Controls, Beijing 100076, People’s Republic of China
E-mail: BIPMC_Wangdy@Outlook.com

Abstract: A safety design method of a civil aircraft cargo door actuation system has been listed in this study in order to fulfil the requirements of airworthiness throughout the product’s life circle, in which a safety design process has been illustrated to show the entire process which will have an impact on the function design. A safety analysis method of fault tree analysis has been chosen to realise the purpose, which is based on the fault modes provided from failure modes and effects analysis and the system reliability prediction results. A design refinement has been made according to the analysis results in order to realise a high safety system.

1 Introduction

Among the most significant criterions of civil aircraft, safety, economy, amenity and so on, safety is the priority that should be considered preliminary, as a result, the safety objective shall be achieved in the design of civil aircraft [1–3]. If certain problems occurred in operation, it may cause severe impact on the life and property of passengers [4]. In order to avoid safety problems, a reasonable safety design method shall be performed throughout aircraft system design [5].

A mechatronic actuator scheme has been used to perform the actuation function of the C919 aircraft cargo door. As a key actuation part of the cargo door system, if the door accidentally opened during flight, it is likely to lead to crash and death for the aircraft [6]. In order to avoid the door accidentally open, it is essential to perform a safety design to avoid security failures.

A series of research related to aircraft safety have been discussed, the safety factors in civil aircraft design requirements have been discussed in [7], the wire failures have been analysed into quantitative safety analysis in [8]; these discussions give the useful information of the safety design in this paper. A preliminary assessment research has been illustrated in [9], which gives an information of how to solve a preliminary design.

The safety design of the cargo door actuation system based on SAE ARP4761, guidelines and methods for conducting the safety assessment process on civil aircraft systems and equipment, which includes the quantitative results of functional hazard assessment (FHA), the analysis of preliminary system safety assessment and system safety assessment which comprising the analysis of failure modes and effects analysis (FMEA) and fault tree analysis (FTA) based on the results of system reliability prediction (SRP). Common mode analysis is performed to verify that the base events in FTA are independent in the actual implementation [10]. The paper using the safety and reliable analysis results to give a feedback for system design, which aimed to realise a high safety as well as a well performance system. The relationship of the analyses of the safety design process is shown in Fig. 1 [11].

2 System overview

Each aircraft has two cargo door actuation systems which are mounted on the front and rear cargo doors. A cargo door actuation system is comprised of three line replaceable units (LRU): a linear actuator (LA), a control panel (CP) and a flexible shaft (FS). The LA is installed between the cargo door of the aircraft and the fuselage structure to open and close the cargo door. The CP is installed on the stressed-skin structure of the aircraft. The FS is used to connect the LA and the CP, when the power is cutting off, the cargo door actuation system can be manually operated through the FS.

The structural block diagram of the cargo door actuation system is shown in Fig. 2. The grey parts represent the three LRUs of the system, the main components are shown in white in diagram. The cargo door actuation system has two control modes: electric mode and manual mode. Ground crew can choose either of them considering of the environment condition from the CP.

In the electric mode, ground crew can operate the door open/close button on the CP, and then the control command can be sent from the CP to the control driver, which can drive the mechatronic
actuator to realise the open/close function. When the opening button is pressed, the actuator will lift the cargo door to the open position and then hold it until received the next control command. The transmission path of the electric mode is when powered on as well as the e-brake received the unlocked signal, the brake can be released then the motor can drive the transmission components to realise the actuation to lift the cargo door. When the door is in holding mode and power is off, if accident move occurred, both no-back and e-brake need to use the backstop function to prevent the movement. When the close button is pressed, the actuator pulls the cargo door back to the closed position [12].

In the manual mode, ground crew input torque at the manual power input end of the CP with the driving tool, and the FS drives the cargo door actuator to extend/retract to realise the open/close action of the cargo door.

3 Safety analysis

System safety assessment is a key link in the safety analysis process of the cargo door actuation system. By doing safety assessment, it is possible to determine how failures in the cargo door actuation system will lead to the failure states identified in FHA and how the quantitative safety objectives and requirements identified in FHA can be met.

The safety assessment of the cargo door actuation system using a method of FTA is based on the results of SRP, FHA and FMEA which can make a decision that whether the safety of the system can meet the safety requirements or not.

The safety assessment of the cargo door actuation system is based on certain assumptions:

(i) In the calculation, prediction and allocation of safety analysis, it is assumed that the system's failure is subjected to an exponential distribution, the failure rate of the exponential distribution is subject to a bathtub curve, inside, the failure rate is divided into early failure stage, accidental failure stage and loss failure stage.

(ii) Software and human operation is completely reliable, failure rate is 0.

(iii) All reliability calculation results are calculated according to MIL-HDBK-217F and NPRD, NSWC.

(iv) A flight duration is 3 h.

(v) The designed monitor provides a 100% effective range of fault detection for functional components.

3.1 Safety requirement

Failure conditions in FHA can be qualitatively divided into two categories, availability failure conditions and integrity failure conditions [10]. Considering the two characteristics in system safety design of the cargo door actuation system, the following failure conditions can be summarised:

(i) Loss of actuation on the ground;
(ii) Accident actuation on the ground;
(iii) Accidental actuation during flight.

Given a qualitative failure rate value decomposed from the cargo door system, the result and preliminary design scheme can be given in Table 1.

A failure condition assessment can be given as follows, for safety requirement 01, loss of actuation on the ground is defined as a class IV failure, which will slightly increase the load of the crew and have no impact on the aircraft and passengers. For safety requirement 02, accident actuation on the ground is defined as a class III failure, which will affect the safety of ground staff. In the initial stage of take-off, the aircraft will be interrupted, which will have a great impact on the aircraft plan, but no impact on the aircraft and passengers. For safety requirement 03, accidental actuation during flight is defined as a class I failure, which will lead to aircraft pressure relief, aircraft structural damage and crash, which will greatly increase the work load of the crew and may cause loss of working ability, results in death or injury of passengers.

As a key part in safety assessment in system design, the FHA results can be used as an input of the whole safety analysis, and each failure condition is placed in the upper level of FTA in Section 3.3.

3.2 Reliability prediction

A preliminary SRP has been performed based on the architecture of the current cargo door actuation system (CDAS) system. The reliability prediction analysis is based on MIL-HDBK-217F, notice 2 for electronic components and NPRD-95, NSWC-98 for the mechanical components. The result of the main functional components of CDAS is shown in Table 2, which is used to provide the fundamental information of the FTA.

3.3 Fault tree analysis

FTA is one of the safety design and evaluation of the probability calculation analysis tools [13, 14] and the FTA method is based on SAE ARP4761, specific events which are not expected to occur in the system can be researched through a deductive fault analysis approach, strictly using fault level to make a causal logic analysis, then the logic diagram can be drawn step by step [15], finally all reasons and causes of the top event in FHA can be found.

The following assumptions are made for the analysis of FTA:

### Table 1 System requirements and preliminary design scheme

| No. | Safety requirements         | Qualitative requirements | Design scheme                        |
|-----|----------------------------|--------------------------|--------------------------------------|
| 01  | loss of actuation on the ground; | less than 1 × 10⁻⁵/FH | design margin BIT common cause analyse |
| 02  | accident actuation on the ground; | less than 1 × 10⁻⁵/FH | design margin (special design using electro-magnetic brake and bi-directional clutch) common cause analyse |
| 03  | accident actuation during flight | less than 1 × 10⁻⁹/FH | common cause analyse                 |

### Table 2 Reliability prediction results

| No. | Name                        | LRU | Failure rate (/H) |
|-----|------------------------------|-----|-------------------|
| 1   | mechanical jam               | LA  | 2 × 10⁻⁶          |
| 2   | FS transmission fault        | FS  | 1.2 × 10⁻⁶        |
| 3   | switch accident actuation    | CP  | 0.2 × 10⁻⁶        |
| 4   | no-back lost function        | LA  | 2.55 × 10⁻⁶      |
| 5   | E-brake lost function        | LA  | 0.88 × 10⁻⁶      |
| 6   | LA transmission structure failure | LA | 0.71 × 10⁻⁶  |
| 7   | FPGA logic failure           | LA  | 1 × 10⁻¹⁰        |
| 8   | power switch abnormal powered | CP | 1 × 10⁻⁶        |
(i) All fault trees assume that the airplane has been dispatched on the current flight with a properly working CDAS and there are no outstanding maintenance actions.

(ii) All fault trees assume that CDAS is manufactured with the correct components properly installed and rigged, and that the components have been determined to be operating within their manufacturer specific tolerances.

(iii) All failure rates are assumed to be constant over the life of the airplane.

The ram commander gates used in this FTA are shown and defined in Fig. 3.

The results of the FTA indicate that the final probability of loss actuation on the ground is $3.2 \times 10^{-6}/H$, which can fulfill the system requirement of 01 in FHA. From the FTA, there exist three combination factors, meantime loss of manual and powered actuation, mechanical jam and FS transmission fault, if any of the three happens, then the CDAS system will lose actuation function.

The FTA of ‘accident actuation on the ground’ is shown in Fig. 5. The results show that the final probability of accident actuation on the ground is $4.54 \times 10^{-6}/H$, which can fulfill the system requirement of 02. There are several factors which influenced the final result, such as failure rate of control command, FPGA logic, transmission structure, the locked function loss of no-back and e-brake. As the reason of the probability has little margin to satisfy the safety requirements, a design improvement need to be made through the CDAS system structure design, the approaches are shown in Section 4.

The FTA of ‘accidental actuation during flight’ is shown in Fig. 6. The result shows that the final probability of accidental actuation during flight is $0.2 \times 10^{-12}/H$, which can fulfill the requirements of SR003 in FHA.

### 4 Design refinement

A conclusion from the above results of FTA can be made that during the safety analysis process, the safety requirement of accident actuation on the ground will be highly concerned. In the previous system design, when in the electric mode, no-back can realise the function of prevent accidental action; when in the manual mode, e-brake can lock the motor shaft to realise the function of prevent accidental action. To realize both the aim of the system function and safety design, a high reliability e-brake can to be chosen to reduce the failure rate as well as a dual redundancy no-back structure is designed to improve system structure, meanwhile, the reliability of electronic components needs to be promised.

For the design of a dual redundancy no-back structure, the new system structure can be shown in Fig. 7. A redundancy no-back (in yellow) is designed inside the CP as a connected part between the...
transmission part and the manual power tool interface. When choosing the electric mode, the CP no-back can promise stop actuation in parallel with the LA no-back, which effectively improve the no-back mechanism's reliability.

In order to reduce the failure rate of the electronic components, in the design process, CDAS system choose the approach to improve the classification of quality as well as conduct the tolerance, derating, protecting circuit and shock-proof designs and other technological measures.

Meanwhile, CDAS system also have an automatic motor speed limit program, and the motor control is designed to provide dynamic braking to limit the speed of the motor to cope with the door in the event that the e-brake fails to hold the door in position.

5 Conclusion
A safety assessment process throughout the cargo door actuation system design development has been listed in this paper using the analysis method of FTA. The results show that a design improvement of the CDAS system has been made throughout the safety design process which is necessary to achieve the safety requirements. After the iterative design, a high safety characteristic can be achieved in the CDAS system.

6 References
[1] Qiang, Q.: ‘Safety and reliability analysis for the doors of civil aircraft’ (Northwestern Polytechnical University, People's Republic of China, 2016)
[2] Cheng, C.: ‘A thesis in safety technology and engineering’, Nanjing University of Aeronautics, 1028707 09-0021
[3] Kelin, Z.: ‘Airworthiness considerations of landing gear control system design of civil aircraft’, Sci. Technol. Innov. Herald, 2011, 29, pp. 42–44
[4] Yunwen, F., Xionghua, Y., Xiaofeng, X., et al.: ‘Research of safety analysis of doors of civil aircraft’, J. Northwestern Polytechnical Univ., 2013, 31, (5), pp. 803–809
[5] Qiaojun, C.: ‘A preliminary aircraft safety assessment research based on aircraft structure’, Sci. Technol. Innov. Herald, 2015, 36, pp. 41–44
[6] Job, M.: ‘Air disaster’ (Aerospae Publications Pty. Ltd., Australia, 2001), vol. 1, pp. 127–144
[7] Brustow, J.W., Irving, P.E.: ‘Safety factors in civil aircraft design requirements’, Eng. Fail. Anal., 2007, 14, pp. 459–470
[8] Guofang, Z.: ‘Study on a safety quantitative analysis method of civil airplane reckoning with wire failures’, Adv. Aeronaut. Sci. Eng., 2012, (3), pp. 241–246
[9] Lei, L.: ‘Research on system preliminary safety assessment of civil aircrafts’, Sci. Technol. Innov. Herald, 2015, 22, pp. 28–29
[10] SAE-ARP4754A REV A: ‘Guidelines for Development of Civil Aircraft and Systems’, SAE Aerospace, December 2010
[11] SAE-ARP4761: ‘Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment’, Society of Automotive Engineers, December 1996
[12] Jian, Y., Zhenjin, N., Xin, W., et al.: ‘Cargo door electromechanical actuation system design on load matching’, Aerosp. Manuf. Technol., 2019, 4, (2), pp. 23–27
[13] Ortmeyer, F., Schellhorn, G.: ‘Formal fault tree analysis-practical experiences’, Electron. Notes Theor. Comput. Sci., 2007, 185, pp. 139–151
[14] Zheng, L.: ‘Design and implementation of fault detection system based on dynamic fault tree’ (Harbin Engineering University, People's Republic of China, 2017)
[15] Dobrivoje, C., Milomir, G., Mile, S., et al. ‘Fault tree analysis of hydraulic power-steering system’, Int. J. Vebl. Des., 2014, 64, (1), pp. 26–45

Fig. 5 FTA of accident actuation on the ground

Fig. 6 FTA of accident actuation during flight

Fig. 7 Figure of system structure improvement